# SmartPass 7.6 User's Guide

Juniper Network, Inc.
1194 N. Mathilda Avenue
Sunnyvale, CA 94089 USA
408-745-2000
www.juniper.net

Part Number: 730-9502-0299 Rev. C

Copyright © 2011, Juniper Networks, Inc. All rights reserved.

## Trademarks

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, T-series, and TX Matrix. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

## Disclaimer

All statements, specifications, recommendations, and technical information are current or planned as of the date of the publication of this document. They are reliable as of the time of this writing and are presented without warranty of any kind, expressed or implied. In an effort to continuously improve the product and add features, Juniper Networks reserves the right to change any specifications contained in this document without prior notice of any kind.

Copyright © 2011, Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, T-series, and TX Matrix. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

# Table of Contents


About This Guide

Chapter 1 Setting Up SmartPass

New Features in SmartPass 7.6 . . . 1-1
Licensing . . . 1-2
SmartPass Licensing . . . 1-2
Guest Access Licensing . . . 1-2
Subscriber Management Licensing . . . 1-2
Security Licensing . . . 1-3
Upgrading the SP 7.6 License . . . 1-3
Obtaining a SmartPass License . . . 1-4
Activating SmartPass Licenses . . . 1-4
Activating a Base License . . . 1-4
Activating Additional SmartPass Licenses . . . 1-4
Setup/Server Settings . . . 1-5
RADIUS Server Settings . . . 1-5
Server Settings and SmartPass Serving Settings . . . 1-5
Server Settings / RADIUS Server Settings . . . 1-5
RADIUS Dynamic Authorization Settings . . . 1-5
External RADIUS Authentication . . . 1-6
Configuring RADIUS Authentication . . . 1-6
Web Portal Authentication Server . . . 1-7
Server Certificate . . . 1-7
Importing the CSR and CA Certificates . . . 1-7
User Roles . . . 1-8
Access Control and Accounts . . . 1-8
Enabling SmartPass Login . . . 1-8
Requiring All SmartPass Users to Log in . . . 1-8
Disabling the Login Requirement (once Enable login-required is turned on) . . . 1-8
Creating and Managing Accounts . . . 1-9
RADIUS-based Login for User Roles . . . 1-9
Creating and Managing Administrator User Accounts . . . 1-9
Creating and Managing Provisioning User Accounts . . . 1-11
Configuring Self-Signed Access Control . . . 1-11
Assigning a Provisioning User to a Self-Signed User Account . . . 1-12
Adding an MX as a RADIUS Client on SmartPass . . . 1-13
Using the Allow any Client Option . . . 1-13
Database (DB) Settings . . . 1-13
Location Appliance Settings . . . 1-15
Location Appliance Settings . . . 1-15
Refresh Locale List . . . 1-15
Coupon Management . . . 1-15
Coupon Enhancements in SmartPass 7.6 . . . 1-15
Coupon Management . . . 1-15

Coupon Template Management . . . . . 1-16
SMTP and SMS Settings . . . . . 1-16
User-Type Configuration Changes . . . . . 1-18
User Configuration Changes . . . . . 1-18
E-mail/Text Message Related Actions . . . . . 1-18
Global Save Coupons Action . . . . . 1-18

## Chapter 2 Web Portal Management

Web Portal Authentication Server . . . . . 2-1
Web Portal Management Page . . . . . 2-1
Web Portal Configuration Wizard . . . . . 2-2
Deleting SSID Configurations . . . . . 2-2
Adding SSID Configurations . . . . . 2-2
Configuring SmartPass as an External Captive Portal Server . . . . . 2-3
Configuring the SmartPass Connection to the MX . . . . . 2-3
Configuring the MX to Support SmartPass . . . . . 2-3
Adding SmartPass Server as a RADIUS Server on the MX (CLI) . . . . . 2-3
Configuring the MX With RingMaster . . . . . 2-4
SmartPass Network Level Setup . . . . . 2-4
SmartPass Wizard . . . . . 2-4
SmartPass Accounting Summary . . . . . 2-5
SmartPass Accounting Details . . . . . 2-6

## Chapter 3 SmartPass Guest Access

MX Configuration . . . . . 3-1
User Groups . . . . . 3-1
Fallthru Authentication . . . . . 3-2
Creating and Managing Users . . . . . 3-2
Creating Custom User Types . . . . . 3-2
Managing User Types . . . . . 3-4
Editing a Custom User Type . . . . . 3-4
Deleting a Custom User Type . . . . . 3-4
Viewing a Custom User Type . . . . . 3-4
Creating and Managing Users . . . . . 3-5
User Types . . . . . 3-5
MAC and Bonded Authentication . . . . . 3-5
Creating Users . . . . . 3-6
Creating Multiple Users at One Time . . . . . 3-6
Creating Multiple Users . . . . . 3-6
Auto-generating User Names . . . . . 3-6
Bulk Create MAC Address Users . . . . . 3-7
Managing Users . . . . . 3-7
Showing User Details . . . . . 3-7
Deleting Users . . . . . 3-7
Disconnecting Users . . . . . 3-8
Unlocking a User . . . . . 3-8

Clearing the MAC Restriction . . . 3-8
Printing a User Report . . . 3-8
Exporting to CSV . . . 3-8
Viewing and Printing Guest Coupons . . . 3-8
Saving Coupons . . . 3-9
E-mailing Coupons . . . 3-9
Texting Coupons . . . 3-9
Printing Single-User Coupons After Creating Users . . . 3-10
Reactivating an Expired User . . . 3-10
Changing a Users Password . . . 3-10
Changing a User Type . . . 3-10
Sessions Monitoring . . . 3-11
Sessions View . . . 3-11
Filtering . . . 3-12
Basic Filters . . . 3-12
Configuring Advanced Filters . . . 3-12
Disconnect Sessions . . . 3-13
Reports . . . 3-13
Accounting Summary Report . . . 3-13
Displaying User Name Report . . . 3-13
Displaying the MAC Address Report . . . 3-14
Table Refresh . . . 3-14

Chapter 4 Network Access Rules

Custom Access Control Rule Example . . . 4-1
Selecting the Conditions Descriptions . . . 4-1
Managing Access Rules . . . 4-2

Chapter 5 RADIUS Proxy

RADIUS Proxy Settings . . . 5-1
Proxy Filters . . . 5-1
Forwarding Conditions . . . 5-1
Forwarding Destination . . . 5-2
RADIUS Server Groups . . . 5-2
RADIUS Server Entries . . . 5-2
Failback Capability . . . 5-2
Default VSA Values . . . 5-3
Realms . . . 5-3
Suffixed Realms . . . 5-3
Prefixed Realms . . . 5-3
User Name Processing . . . 5-3
Access Rule Integration . . . 5-3
Granting Access . . . 5-4
Denying Access . . . 5-4
Compatibility . . . 5-4
RADIUS Proxy Tab . . . 5-4
RADIUS Proxy Settings . . . 5-4

RADIUS Servers Management . . . . . 5-5
Creating a RADIUS Server . . . . . 5-5
Editing a RADIUS Server Entry . . . . . 5-5
Creating a RADIUS Server Group . . . . . 5-5
Deleting a RADIUS Server Entry . . . . . 5-5
RADIUS Proxy Rules Management Page . . . . . 5-5
Creating a RADIUS Proxy Rule . . . . . 5-5
Template /Custom Rule . . . . . 5-6
The Rule Conditions Page . . . . . 5-6
User Name Pattern . . . . . 5-6
The AP MAC Address Selection . . . . . 5-6
Selecting a Realm . . . . . 5-6
The Destination Page . . . . . 5-6
The Default Attributes Page . . . . . 5-7
The Description Page . . . . . 5-7

Chapter 6 Maintaining SmartPass

Exporting Log Files . . . . . 6-1
Database Backup and Restore . . . . . 6-2
Auto-Backup . . . . . 6-2
Creating a Manual Backup of the Database . . . . . 6-3
Backups Management . . . . . 6-3

# About This Guide

## SmartPass 7.6 User's Guide

This guide is intended for network administrators or persons responsible for installing and managing SmartPass 7.6 software.

## 7.6 API User Guide

SmartPass provides a fully functional REST-based web API that can be used to integrate the data stored in SmartPass with any third party system. The API is described in the SmartPass API Reference Guide.

Internally, RingMaster manages the reporting for the accounting data stored in the SmartPass accounting tables. The actual reporting is performed within RingMaster and the data is provided by SmartPass via an API.

## RingMaster Publication Suite

SmartPass 7.6 is used with RingMaster (versions 6.2 and higher)and allows you to configure SmartPass as an accounting as well as a DAC server and also generate client session reports based on accounting information collected by the *SmartPass* server.

Publications that make up the *Ringmaster* Publication Suite are:

- *RingMaster 7.6 Quick Start Guide* — This guide provides a description of prerequisites and procedures required to install and begin using RingMaster 7.6 software. Information is provided about system requirements for optimum performance, as well as how to install RingMaster Client and RingMaster Services software.
- *RingMaster Planning Guide* — This guide provides instructions for planning a WLAN with the *RingMaster* tool suite.It describes RingMaster 7.6 planning tools. It is intended for network administrators or persons responsible for planning a WLAN using RingMaster 7.6 software.
- *RingMaster Configuration Guide* — This guide provides detailed procedures for configuring a Wireless Local Area Network (WLAN) using RingMaster 7.6 software.
- *RingMaster Management Guide* — This guide provides instructions for managing a WLAN with the RingMaster tool suite. It describes RingMaster 7.6 WLAN management and monitoring tools. It is intended for administrators of WLANs using RingMaster 7.6 software.

## Mobility System Configuration and Management

SmartPass 7.6 is used with Juniper Networks Mobility System hardware and software, as described in the following publications:

- *Juniper Networks Mobility System Software Configuration Guid*e — This guide provides instructions for configuring and managing a system using the Juniper Networks Mobility System Software (MSS) Command Line Interface (CLI).
- *Juniper Networks Mobility System Software Command Reference* — This publication provides functional and alphabetic reference to all MSS commands supported on MXs and MPs
- *Juniper Networks Mobility Exchange Hardware Installation Guide* — Instructions and specifications for installing an MX.
- *Juniper Networks Mobility System Software Quick Start Guide* — Instructions for performing setup of secure (802.1X) and guest (WebAAA™) access, and configuring a Mobility Domain for roaming

Copyright © 2011, Juniper Networks, Inc.

- *Juniper Networks Mobility Point MP-422 Installation Guide* — Instructions and specifications for installing an MP access point and connecting it to an MX.
- *Juniper Networks Mobility Point MP-620 Installation Guide* — Instructions and specifications for installing the MP-620 access point and connecting it to an MX.
- *Juniper Networks Regulatory Information* — Important safety instructions and compliance information that you must read before installing Juniper Networks products

## Juniper Networks Documentation Conventions

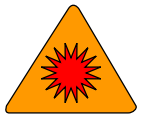
### Safety and Advisory Notices

The following types of safety and advisory notices appear in this guide.

This is an Electrostatic Discharge warning.

This is a frame ground message.

This is a Laser warning.



This is a protectrive ground message.

This situation or condition can lead to data loss or damage to the product or other property.

Copyright © 2011, Juniper Networks, Inc.

This is a process or procedural tip or other useful suggestion.

This information you should note relevant to the current topic.

This alerts you to a possible risk of personal injury or major equipment problems.

## Hypertext Links

Hypertext links appear in Blue.

As an example, this is a link to **Contacting the Technical Assistance Center**.

## Text and Syntax Conventions

Juniper Networks guides use the following text and syntax conventions:

| Convention | Use |
|---|---|
| Monospace text | Sets off command syntax or sample commands and system responses. |
| **Bold text** | Highlights commands that you enter or items you select. |
| *Italic text* | Designates command variables that you replace with appropriate values or highlights publication titles or words requiring special emphasis. |
| Bold italic text font | Bold italic text font in narrative, capitalized or not, indicates a program name, function name, or string. |
| **Menu Name** > **Command** | Indicates a menu item. For example, **File** > **Exit** indicates that you select **Exit** from the **File** menu. |
| [ ] (square brackets) | Enclose optional parameters in command syntax. |
| { } (curly brackets) | Enclose mandatory parameters in command syntax. |
| \| (vertical bar) | Separates mutually exclusive options in command syntax. |

For information about Juniper Networks support services, visit http://www.juniper.net/, or call 1-866-877-9822 (in the US or Canada) or +1 925-474-2400 and select option 5.

Juniper Networks sells and services its products primarily through its authorized resellers and distributors. If you purchased your product from an authorized Juniper Networks reseller or distributor and do not have a service contract with Juniper Networks, you must contact your local reseller or distributor for technical assistance.

Copyright © 2011, Juniper Networks, Inc.

## Contacting the Technical Assistance Center

Contact the Juniper Networks Technical Assistance Center (TAC) by telephone, email, or via web support portal.

- Within the US and Canada, call 1-866-TRPZTAC (1-866-877-9822).
- Within Europe, call +31 35 64 78 193.
- From locations outside the US and Canada, call +1 925-474-2400.
- In non-emergencies, send email to http://www.juniper.net/
- If you have a service contract or are a Juniper Networks Authorized Partner, log in to http://www.juniper.net/ to create a ticket online.

### TAC Response Time

TAC responds to service requests as follows:

| Contact method | Priority | Response time |
|---|---|---|
| Telephone | Emergency | One hour |
| | Non-emergency | Next business day |
| Email | Non-emergency | Next business day |

### Information Required When Requesting Service

To expedite your service request, please have the following information available when you call or write to TAC for technical assistance:

- Your company name and address
- Your name, phone number, cell phone or pager number, and email address
- Name, model, and serial number of the product(s) requiring service
- Software version(s) and release number(s)
- Output of the *show tech-support* command
- Wireless client information
- Description of any problems and status of any troubleshooting effort

# Warranty and Software Licenses

Current Juniper Networks warranty and software licenses are available at http://www.juniper.net/.

## Limited Warranty for Hardware and Software

TERMS AND CONDITIONS OF SALE

1. Software

   Any software provided is licensed pursuant to the terms and conditions of Juniper Network's Software License Agreement, an electronic copy of which is provided with the software ("Software License Agreement") and a printed copy of which is available upon request. The Software License Agreement is incorporated by this reference into these Terms and Conditions of Sale (collectively referred to as "Terms and Conditions of Sale"). In the event of any conflict between the Software License Agreement and these Terms and Conditions of Sale, the Software License Agreement shall control, except for the terms of the limited hardware and software warranty set forth below ("Limited Warranty").

2. Limited Hardware Warranty

Juniper Networks, Inc. ("Juniper Networks") warrants solely to Customer, subject to the limitation and disclaimer below, that all Juniper Networks hardware will be free from defects in material and workmanship under normal use as follows: (a) if the hardware was purchased directly from Juniper


Copyright © 2011, Juniper Networks, Inc.

Networks, for a period of one (1) year after original shipment by Juniper Networks to Customer, (b) if the hardware was purchased from a Juniper Networks Authorized Distributor or Reseller, for a period of one (1) year from the date of delivery to Customer, but in no event more than fifteen (15) months after the original shipment date by Juniper Networks, or (c) for certain indoor Mobility Point® access points that are specifically identified on Juniper Network's price list for the lifetime of the hardware (each of the foregoing, the "Limited Hardware Warranty"). The date of original shipment from Juniper Networks will be determined by shipping evidence on file at Juniper Networks. This Limited Hardware Warranty shall not apply to any third party products provided under this Agreement which shall be subject exclusively to the manufacturers warranty for such products and extends only to the Customer who was the original purchaser of the hardware and may not be transferred to any subsequent repurchasing entity. During the Limited Hardware Warranty period upon proper notice to Juniper Networks by Customer, Juniper Networks will, at its sole option, either:

- Repair and return of the defective hardware;
- Replace the defective hardware with a new or refurbished component;
- Replace the defective hardware with a different but similar component that contains compatible features and functions; or
- Refund the original purchase price paid upon presentation of proof of purchase to Juniper Networks.

**3.** Restrictions on the Limited Hardware Warranty.

This Limited Hardware Warranty does not apply if the hardware (a) is altered from its original specifications, (b) is installed, configured, implemented or operated in any way that is contrary to its documentation, (c) has damage resulting from negligence, accident, or environmental stress, (d) was subject to unauthorized repair or modification, or (e) is provided to Customer for pre-production, evaluation or charitable purposes.

**4.** Limited Software Warranty

Juniper Networks warrants solely to Customer, subject to the limitation and disclaimer below, that the software will substantially conform to its published specifications as follows: (a) if the software was purchased directly from Juniper Networks, for a period of ninety (90) days after original shipment by Juniper Networks to Customer, or (b) if the software was purchased from a Juniper Networks Authorized Distributor or Reseller, for a period of ninety (90) days from the date of delivery to Customer commencing not more than ninety (90) days after original shipment date by Juniper Networks), ("Limited Software Warranty"). The date of original shipment from Juniper Networks will be determined by shipping evidence on file at Juniper Networks. This Limited Software Warranty shall not apply to any third party products provided under this Agreement which shall be subject exclusively to the manufacturers warranty for such products and extends only to the Customer of original purchaser of the software and may not be transferred to any subsequent repurchasing entity.

During the Limited Software Warranty period upon proper notice to Juniper Networks byCustomer, Juniper Networks will, at its option, either:

- Use reasonable commercial efforts to attempt to correct or provide workarounds for errors;
- Replace the software with functionally equivalent software; or
- Refund to Customer the license fees paid by Customer for the software.

Juniper Networks does not warrant or represent that the software is error free or that the software will operate without problems or disruptions. Additionally, and due to the steady and ever-improving development of various attack and intrusion technologies, Juniper Networks does not warrant or represent that any networks, systems or software provided by Juniper Networks will be free of all possible methods of access, attack or intrusion.

**5.** Restrictions on the Limited Software Warranty

Copyright © 2011, Juniper Networks, Inc.

This Limited Software Warranty does not apply if the software (a) is altered in any way from its specifications, (b) is installed, configured, implemented or operated in any way that is contrary to its documentation, (c) has damage resulting from negligence, accident, or environmental stress, (d) was subject to unauthorized repair or modification, or (e) is provided to Customer for pre-production, evaluation or charitable purposes

**6.** General Warranty Disclaimer

EXCEPT AS SPECIFIED IN THIS LIMITED WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR APPLICATION OR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE AFOREMENTIONED WARRANTY PERIOD. BECAUSE SOME STATES, COUNTRIES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM JURISDICTION TO JURISDICTION. THE LIMITED WARRANTY ABOVE IS THE SOLE REMEDY FOR ANY BREACH OF ANY WARRANTY WITH RESPECT TO THE HARDWARE AND SOFTWARE AND IS IN LIEU OF ANY AND ALL OTHER REMEDIES.

**7.** Limitation of Liabilities

IN NO EVENT SHALL JUNIPER NETWORKS, ITS SUPPLIERS, OR ITS AUTHORIZED DISTRIBUTORS OR RESELLERS BE LIABLE TO CUSTOMER OR ANY THRID PARTY FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES REGARDLESS OF HOW THOSE DAMAGES WERE CAUSED. NOR WILL JUNIPER NETWORKS, ITS SUPPLIERS, OR ITS AUTHORIZED RESELLERS BE LIABLE FOR ANY MONETARY OR PUNITIVE DAMAGES ARISING OUT OF THE USE OF, OR INABILITY TO USE JUNIPER NETWORKS HARDWARE OR SOFTWARE. JUNIPER NETWORK'S LIABILITY SHALL NOT EXCEED THE PRICE PAID BY THE CUSTOMER FOR ANY HARDWARE OR SOFTWARE COVERED UNDER THE TERMS AND CONDITIONS OF THIS WARRANTY. THIS LIMITATION OF LIABILITY AND RESTRICTION ON DAMAGES APPLIES WHETHER IN CONTRACT, TORT, NEGLIGENCE, OR OTHERWISE, AND SHALL APPLY EVEN IF THE LIMITED WARRANTY FAILS OF ITS ESSENTIAL PURPOSE. WARRANTY LAWS VARY FROM JURISDICTION TO JURISDICTION, AND THE ABOVE LIMITATIONS AND EXCLUSION OF CONSEQUENTIAL AND INCIDENTAL DAMAGES MAY NOT APPLY TO YOU, DEPENDING UPON YOUR STATE, COUNTRY OR JURISDICTION.

**8.** Procedures for Return of Hardware or Software under the Limited Warranty

Where repair or replacement is required under the Limited Warranty, Customer will contact Juniper Networks and obtain a Return Materials Authorization number ("RMA Number") prior to returning any hardware and/or software, and will include the Juniper Networks RMA Number on all packaging. Juniper Networks will ship repaired or replacement components within a commercially reasonable time after receipt of any hardware and/or software returned for the Limited Warranty purposes to the address provided by Customer. Customer will pay freight and handling charges for defective return to the address specified by Juniper Networks and Juniper Networks will pay freight and handling charges for return of the repair or replacement materials to Customer.

**9.** Miscellaneous

These Terms and Conditions of Sale and Limited Warranty shall be governed by and construed in accordance with the laws of the State of California without reference to that State's conflict of laws rules and as if the contract was wholly formed within the State of California. Customer agrees that jurisdiction and venue shall be in Santa Clara County, California. Under no circumstances shall the United Nations Convention on the International Sale of Goods be


Copyright © 2011, Juniper Networks, Inc.

considered for redress of grievances or adjudication of any warranty or other disputes that include Juniper Networks hardware or software. If any provision of these Terms and Conditions of Sale are held invalid, then the remainder of these Terms and Conditions of Sale will continue in full force and effect. Where a Customer has entered into a signed contractual agreement with Juniper Networks for supply of hardware, software or services, the terms of that agreement shall supersede any terms contained within this Terms and Conditions of Sale and Limited Warranty. Customer understands and acknowledges that the terms of this Terms and Conditions of Sale and Limited Warranty, as well as material information regarding the form, function, operation and limitations of Juniper Networks hardware and software will change from time to time, and that the most current revisions will be publicly available at the Juniper Networks corporate web site (http://www.juniper.net/).

Copyright © 2011, Juniper Networks, Inc.

Copyright © 2011, Juniper Networks, Inc.

# Setting Up SmartPass

This chapter describes the tasks required to configure SmartPass, and provides you with step-by-step instructions detailing each task.

## New Features in SmartPass 7.6

SmartPass has evolved into a software tool that gives an IT manager full control over client access to WiFi networks. The network manager can fine tune access and authorization on the wireless LAN both for primary Users and Users on the network. With SmartPass, you not only allow or deny access but also change authorization attributes in response to conditions that change including location, time of day, and amount of traffic per user.

SmartPass 7.6 policies can be defined to match criteria, including SSID, username patterns, VLAN information, location and time of day. Conditions are matched to triggers (updates) received in the authentication, accounting, roaming, and location update data and can be used to either disconnect or alter the authorization attributes of the user. The changes in attributes can be changes on the Access Control Lists (ACL) applied to the user session or applied in the QoS parameters of the session. In addition to access control, SmartPass 7.6 provides enhanced per user reporting and integration with Juniper Network's location appliance, the LA-200.

The following new features are available in SmartPass 7.6:

- **External RADIUS Authentication** - RADIUS Proxy is the ability for a RADIUS server to seamlessly forward RADIUS authentication requests to an external RADIUS server, retrieve the authentication response, optionally post-process any authorization attributes, and send them back to the NAS. SmartPass specific intelligence (such as client location) has been added to the authentication response received from another RADIUS server, by leveraging its existing Access Rule framework.
- **Web Portal Authentication Server** - As an Administrator, you can use this feature to assign an authentication page to a specific SSID. This 7.6 SmartPass feature only works in conjunction with MXs running MSS 7.0 or later.
- **Coupon Enhancements** - You can now e-mail (secure SMTP) or text authentication information or coupons to users.
- **User Notification Settings** - New SMS and E-mail notification capabilities are available.
- **User-Type Configuration Changes for User Account Notification** - Authorization attributes and account notification information and attributes can be configured per User.
- **E-mail/Text Message Related Actions** - New e-mail and text message actions have to added to drop down Actions lists for use during User creation.
- **Create User -** New fields are available on the account creation page for e-mail, phone number, SMS, and company name.
- **Bulk Create Users** - You can associate an E-mail Address or Mobile Phone Number to each user at the time the User is created or edit an existing User to include contact information. The Import Users from CSV mode has been expanded to include E-mail address, phone number, person name, and company name for e-mail and text capabilities.
- **Logging** - Each time a coupon is e-mailed or sent as SMS to a user/group of users, the event is logged under a new Coupons module.
- Licensing - New and improved licensing scheme.

Copyright © 2011, Juniper Networks, Inc.

# Licensing

## SmartPass Licensing

The new licensing scheme used by SmartPass 7.6 includes new SKUs that are more functional and solution based.

SmartPass 7.6 SKUs:

- Guest Access
- Subscriber Management
- Security
- SmartPass Evaluation licenses (SP-EVAL)

  SP-EVAL licenses have all SmartPass 7.6 functionalities available for 50 users and are valid for 90 days from activation.

## Guest Access Licensing

The Guest Access License allows the Administrator, Provisioner and Self-Signed User roles to provision guest access, create custom user types, upload bulk users and access the API calls that are specific to that function.

| SKU | Version 7.1 or earlier equivalent SKU (transition) | Comments / Description |
|---|---|---|
| SP-GA-Base SP | SP | SmartPass Guest Access Base License; Includes 50 guest accounts |
| SP-GA-50 | | SmartPass Guest Access License for additional 50 guests; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier) |
| SP- GA-100 | | SmartPass Guest Access License for additional 100 guests; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier) |
| SP-GA-500 | | SmartPass Guest Access License for additional 500 guests; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier) |
| SP-GA-2500 | | SmartPass Guest Access License for additional 2500 guests; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier) |

User license counts are performed during upgrades to ensure that the number of SmartPass users does not exceed the set number of users in a specific license. Error messages alert you if the maximum numbers of users is exceeded when adding new users.

## Subscriber Management Licensing

Subscriber Management licenses allow you to have functionality in the guest access bundle and in the new external Web Portal Authentication capabilities. The RADIUS proxy feature and


Copyright © 2011, Juniper Networks, Inc.

accounting features are also available as part of this license, including the WEP API operations that are required by RingMaster for Accounting reports.

| SKU | Version 7.1 or earlier equivalent SKU (transition) | Comments / Description |
|---|---|---|
| SP-SM-UPGR | | SmartPass Subscriber Management Base License; Used to upgrade from SP-GA-xx to SP-SM-xx with same user count |
| SP-SM-50 | | SmartPass Subscriber Management License for additional 50 accounts; requires current / previous purchase of SP-GA-BASE, or SP (SmartPass 7.1 and earlier) |
| SP- SM-100 | | SmartPass Subscriber Management License for additional 100 accounts; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier) |
| SP-SM-500 | | SmartPass Subscriber Management License for additional 500 accounts; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier) |
| SP-SM-2500 | SP-ENT | SmartPass Subscriber Management License for additional 2500 accounts; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier) |

### Security Licensing

The SmartPass Security license allows you to have extended user access control and provides accounting RADIUS proxy capabilities so you can track user activity details. The base license is the SP (a license available in releases prior to 7.6) or the SP-GA-BASE. The maximum number of users that can be in the database is 10,000.

| SKU | Version 7.1 or earlier equivalent SKU (transition) | Comments / Description |
|---|---|---|
| SP-SEC-ADV | SP-ACC | SmartPass Advanced Security Feature License; Includes location (LA-200/LA-200E) integration; Dynamic Access Control based on Network Usage, User Identity and Location; requires the current / previous purchase of SP-GA-BASE, SP (SmartPass 7.1 and earlier) |

#### SP-SEC-ADV

The advanced security license is a SmartPass security feature that allows integration with the Location Appliance-200 (LA-200) platform. This is the only difference between the Advanced and Basic security license types. The SP-SEC-ADV license and the SP 7.1 SP-ACC license both allow you to set access rules on the Location Appliance platform.

## Upgrading the SP 7.6 License

### Upgrading the License Feature Set and User Count

It is important that you use the SP-SM-UPGR license to upgrade a SP-GA-XX license to a SP-SM-XX license. The features offered in the Subscriber Management license are activated only after installation of the SP-SM-XX license.

### Upgrading Only the Feature Set

If you are upgrading from SP-GA-XX to SP-SM-XX, you need to install SP-SM-UPGR to go from Guest Access to Subscriber Management functionality. The user count on the upgraded SP-SM-xx license can be increased by adding new user counts to the existing SP-GA-xx license.

Copyright © 2011, Juniper Networks, Inc.

If you are a new customer and want only Subscriber Management functions, then you can install the SP-SM-UPGR license to activate the features without increasing the user count.

### Downgrading the License Set

Once SP-SM-XX licenses are installed the SmartPass server no longer accepts SP-GA-XX licenses.

### Upgrading from a Previous Version of SmartPass

License upgrades from SmartPass 7.0 or 7.1 versions to SP 7.6 licenses are as follows:

- SP is interpreted as SP-GA-BASE
- SP-ENT is interpreted as SP-SM-2500
- SP-ACC is interpreted as SP-SEC-ADV

If you have SP-ACC installed then you receive SP-GA-BASE, SP-SM-2500 and SP-SEC-ADV because the SP-ACC requires SP and SP-ENT licenses.

SmartPass license upgrades do not take place when upgrading SmartPass to 7.6. If you upgrade the SP application without an upgraded license the license file retains SP 7.0 or 7.1 licenses.

Downgrading to an Earlier Version of SmartPass
Downgrading from SmartPass 7.6 to 7.1 or 7.0 requires manual TAC intervention.

## Obtaining a SmartPass License

SmartPass is shipped with a Base License and upgrades may be obtained by contacting your authorized Juniper Networks reseller or partner.

Your Juniper Networks SmartPass software serial number may be found on the original shipping box and on the CD case.

When you upgrade your license, you receive an Upgrade Coupon that contains a new serial number.

To Upgrade and Activate your new license online:

1. Open a browser window and go to http://www.trapezenetworks.com/support/product_licenses.
2. Click on **Generate a SmartPass license key**.
3. Complete the online form.
4. Click **OK**. Your SmartPass License Key is sent to the e-mail address provided in the online form on the License site.

## Activating SmartPass Licenses

### Activating a Base License

After installing SmartPass, you are be prompted to enter your serial number and license key.

### Activating Additional SmartPass Licenses

After you have obtained an additional license and key, you can use the following procedure to apply and activate the license.

To apply and activate a new SmartPass license:

1. Login as an Administrator.
2. Go to **Setup > Licensing**.


Copyright © 2011, Juniper Networks, Inc.

3. Enter the new serial number and license key in the corresponding fields under the **Enter new license** heading.
4. Click **Save**. SmartPass attempts to contact the Juniper Networks licensing server via the Internet and validate your serial number and key. When the process is successful, your new license information appears under the Current Licenses heading.

# Setup/Server Settings

You can configure server ports for SmartPass functionality including the HTTPS Web port and the RADIUS port setting for authentication and accounting. You can also configure port settings for Dynamic Authorization Clients.

## RADIUS Server Settings

### Server Settings and SmartPass Serving Settings

- Configure the port used for Web access to the SmartPass server by entering the port number in the **HTTPS Port** field. Defaults are shown in the screenshot above.

### Server Settings / RADIUS Server Settings

- Configure the authentication port for the RADIUS server by entering the number of the port in the **Authentication Port** field
- You can enable or disable accounting for a specific user by selecting **Enable RADIUS Accounting** in the RADIUS Accounting Settings section.
- There is a configurable **Port** that receives the accounting messages. The default port used for accounting is 1813.
- The **Update Interval (sec)** field allows you to specify the time interval between updated accounting packets. The time is shown in seconds and the default value is 1000 seconds, although the you can enter any time amount between 60 and 3600 seconds This is applicable for users authenticating through SmartPass.

## RADIUS Dynamic Authorization Settings

This feature allows Administrators to disconnect a user or change the authorization attributes of an existing user session. SmartPass uses new terminology in support of RFC 3576 (Dynamic RADIUS) Change of Authorization or Disconnect Message.

- **Dynamic Authorization Client (DAC)** — The component sending the Disconnect and Change of Attribute (CoA) requests to the DAS. Though the DAC often resides on the RADIUS server, it can be located on a separated host, such as a rating engine. In this case, the SmartPass Server acts as a DAC.
- **Dynamic Authorization Server Port** — The UDP port that listens for Acknowledgement (ACK) and Negative Acknowledgement (NAK) requests sent by the DAS. In this case the MX is the DAS.
- **Dynamic Authorization Server (DAS)** — The component residing on the NAS that processes the Disconnect and Change-of-Authorization (CoA) requests sent by the Dynamic Authorization Client (DAC).
  - You can chose to enable or disable the Dynamic authorization service by selecting **Enable Dynamic Authorization** in the RADIUS Dynamic Authorization Settings section.

You can also enter a configurable **Port** number to receive the RFC 3576 messages. The default Dynamic Authorization port is 3799.

Copyright © 2011, Juniper Networks, Inc.

## External RADIUS Authentication

The 7.6 External RADIUS feature is available with all SmartPass licenses. If RADIUS Authentication is enabled, user credentials are checked against the local database when attempting to login to SmartPass. If the User is found, SmartPass performs a local authentication. If not, an authentication request is sent to an external RADIUS Server that checks and then validates or invalidates the credentials. If the credentials are invalid, the External RADIUS Server replies with a reject message and SmartPass displays a log-in failure page. The authentication also fails if none of the RADIUS Servers in your group is reachable.

If the authentication is successful, the External RADIUS Server sends an Access Accept response. The response message provides you with the following authorization attributes:

- User Role
- Assigned User-Types (for Provisioning and Self-Signed Users)
- Assigned Self-Signed Users (for Provisioning Users).

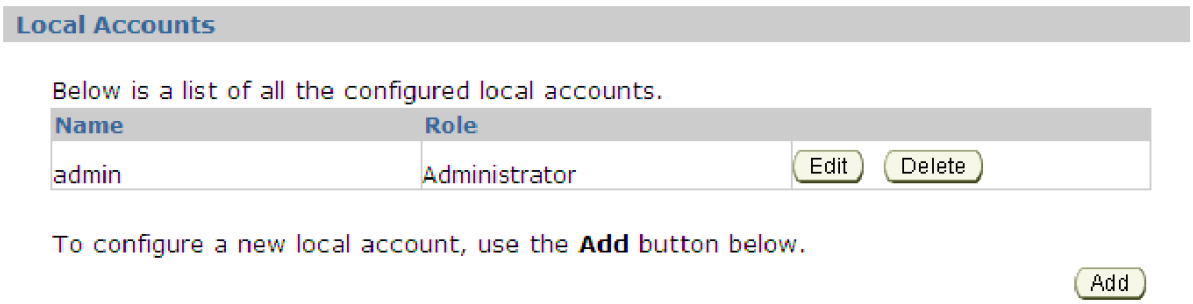
The External RADIUS Server needs to include a minimum of one and up to three Juniper Networks Vendor-Assigned Attribute (VSAs) in the Access Accept response, one for each authorization attribute. The VSA number for RADIUS-based logins is 17. If the VSAs are missing from the response packet and no default user role is selected then authorization is denied.

The VSA attribute value must follow the pattern below:

- The first VSA value (User Role) must be one of the following values: "Administrator","Provisioning" or "Self-Signed." The attribute value is not case sensitive.
- The second VSA value (Assigned User Types) must contain a list of User type names, separated by a semicolon. This VSA is considered only if the first VSA has a value of "Provisioning" or "Self-Signed". Otherwise, it is ignored.
- The third VSA value (Assigned Self Signed Users) must contain a list of self-signed User names, separated by semicolon (;). This VSA is considered only if the first VSA is "Provisioning".

## Configuring RADIUS Authentication

You can add local users to SmartPass with an **Add** button under Access Control, and then **Local Accounts**.





Copyright © 2011, Juniper Networks, Inc.

An updated section named External RADIUS Authentication has been added at the end of the Access Control page. External RADIUS Authentication has the following components:

- Enabled External RADIUS Authentication - disabled by default.
- Authentication Type - a drop down list shows the available authentication methods (PAP and MSCHAPv2). The default value is MSCHAPv2.
- RADIUS Server Group - a drop down list allows you to select an existing RADIUS Server Group. By default no value is selected.
- Default User role - a drop down list that allows you to select the User role to be assigned if the attribute is missing from the incoming Access Response. The default selection is "None."

Default assigned User-types - a drop down list with multiple selections allows you to select an assigned User-type if this attribute is missing from the incoming Access Response. By default, no User-type is selected.

## Web Portal Authentication Server

This feature allows Administrators to allow the users to authenticate locally on the SmartPass database or via an external RADIUS server (configured as a RADIUS proxy).

## Server Certificate

A **Server Certificates Management** section has been added under the Setup menu.

The **Server Certificates Management** section allows you to switch between the DER encoded certificates and PKCS#12 encoded certificates. You can control the options used to upload the PKCS#12 certificate file and to provide the certificate file password. Before you can import the PKCS#12 certificate file, you have to have the certificate in the correct format or the import fails.

This page has two sections:

- **Certificate Signing Request** - SmartPass can generate Certificate Signing Requests that are submitted to certificate authorities. Certificate authorities must sign the generated requests in order for a return certificate or certificate chain to be issued and then uploaded into SmartPass.
- **Server Certificate** - The Server Certificate section contains the controls to switch between the DER encoded certificates and PKCS#12 encoded certificates. There are also options that allow you to upload the PKCS#12 certificate file and others that provide the certificate file password.

1. In the **Certificate Signing Request** (**CSR**) section you can use multiple options to specify the fields that are required by the CSR generation process. Click on **Generate CSR** and enter your information. Common Name is a mandatory field. If no common name is added, then an error message displays.
2. Click on **Create Key Pair** to create an entry with your supplied information. You are provided the CSR in PKCS#10 format inside a read-only text area. A link to the CSR text file is also be displayed which can be used to save the CSR. By default the CSR file is stored in the SP_INSTALL_DIR/sp_cert_req.txt file. SmartPass can only store one CSR at a time. When a new CSR is generated the contents of the previous file is overwritten.

   Your CSR is added to the .services_keystore SmartPass keystore as sp_generated_keypair.

   After the CSR is submitted the request for a server certificate or certificate chain is issued to the Certificate Authority (CA). When the CA signs the CSR and issues a CA certificate, you can use the dedicated upload controls (found in the Certificate Signing Request section of the Server Certificates Management page) to add both certificates to the keystore.

### Importing the CSR and CA Certificates

Before you can import the certificates into SmartPass you must first encode the certificate files issued by the CA into a format accepted by the Java's platform JKS - Java Key Store.

1. Go to the CA's UI. For example: http://172.31.229.4/certsrv/.

Copyright © 2011, Juniper Networks, Inc.

2. Request a certificate.
3. Submit an advanced certificate request.
4. Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file. - this is where you input the CSR issued by SmartPass.
5. Choose one of the following: Certificate Template: Web Server or Certificate Template: Web Server with Private Key.
6. Choose the Base 64 encoded option for the certificates encoding.
7. Download the certificate as file: CERT_NAME.p7b

Use OpenSSL for transforming the PKCS#7 certificate files encoding to the X509/DER format:

1. pkcs7 -print_certs -in CERT_NAME.p7b -out CERT_NAME.cer
2. x509 -in CERT_NAME.cer -inform PEM -out CERT_NAME.der -outform DER

The same code transformation also applies for the CA's certificate.

# User Roles

SmartPass has three categories of users:

- **Administrators** — Access to all the menu tabs and features of SmartPass. They can create other users, set or change user passwords, print coupons, perform all administrative tasks, and create User types.
- **Provisioning Users** — Provisioning Users can view, create, and re-activate Users, as well as change passwords. Provisioning Users are isolated from each other and cannot view or edit Users created by another Provisioning User. This feature provides an additional layer of security.
- **Self-Signed User** — A user role that is available for customers to log into and have Guests create Guest accounts. The Self -Signed user is associated with one or more user-types and one or more provision roles by the Administrator.
- **Guest Users** — Also known as Users, Guest Users have no access to SmartPass. The SmartPass application is used to grant Guest Users access to the corporate wireless network.

# Access Control and Accounts

## Enabling SmartPass Login

SmartPass allows you to control user access and available features based on the role of the user. There are three available roles:

- Administrator
- Provisioning User
- Self-Signed User

## Requiring All SmartPass Users to Log in

1. Launch SmartPass.
2. Click **Setup > Access Control.**
3. Select **Enable login-required**.

## Disabling the Login Requirement (once Enable login-required is turned on)

1. Launch SmartPass.
2. Login as an Administrator.


Copyright © 2011, Juniper Networks, Inc.

3. Click **Setup > Access Control**.
4. Select **Allow All**.

## Creating and Managing Accounts

Administrators may create and manage other Administrators, Provisioning Users, Self-Signed and User accounts.

### RADIUS-based Login for User Roles

Since SmartPass is used both as a Web Portal Authentication Server and a RADIUS server you must separate and secure access to these two different functions of SmartPass.

This can be done through the use of well configured access filters. Requests are filtered so that requests are sent only from the configured NAS clients list.

You can disable the Web Portal Authentication Server functionality via the SmartPass RADIUS Client Settings and Access Rules pages. The enable-login required feature of the RADIUS SmartPass server should be on by default. If web portal is enabled and Enable login is not enabled a warning message on the Server Settings displays. Enabling the Web Portal Authentication service allows external access to SmartPass.

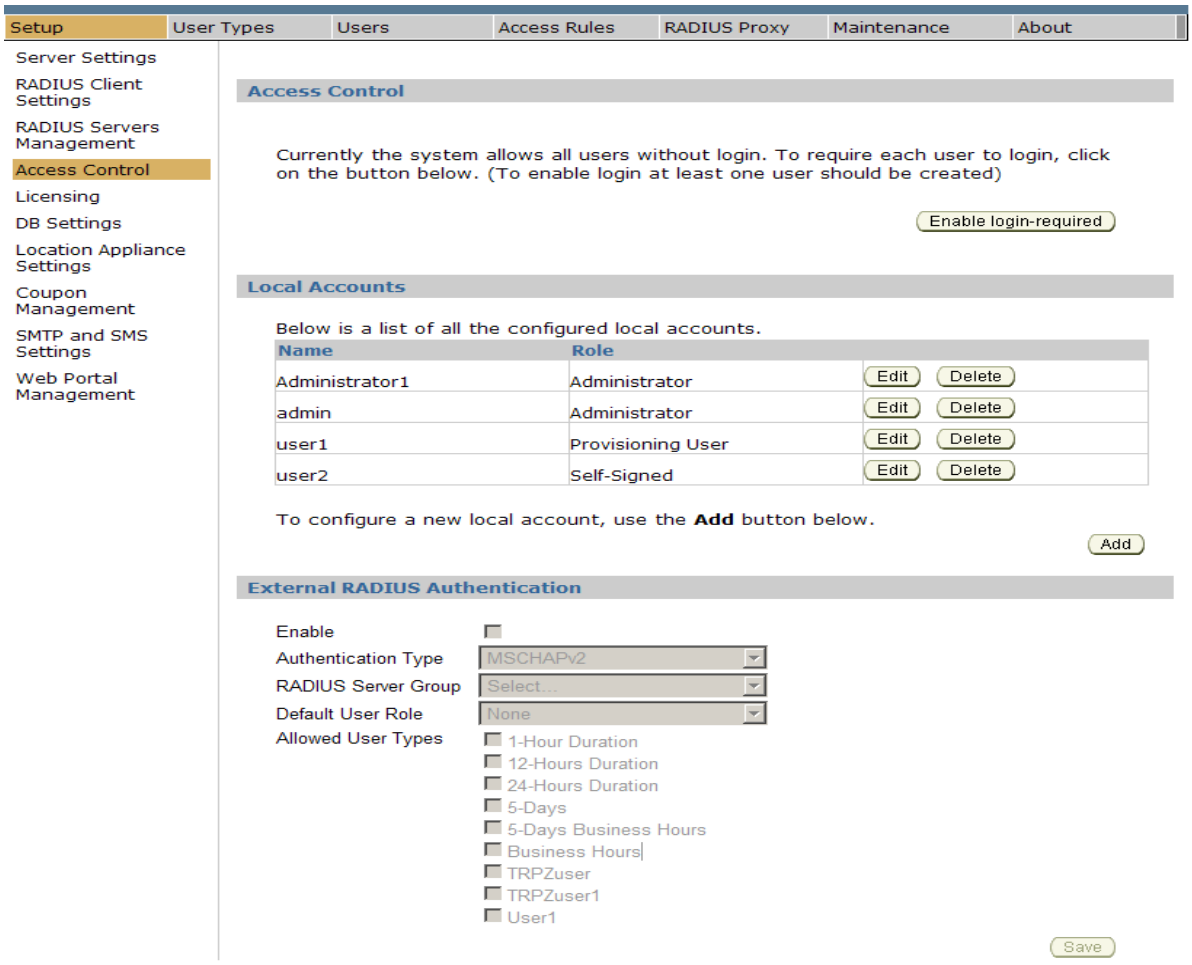
For more information on RADIUS-based logins see Chapter 4, Network Acess Rules.

### Creating and Managing Administrator User Accounts

To create an Administrator Account:

Copyright © 2011, Juniper Networks, Inc.

1. Go to **Setup > Access Control**.




2. Click **Add**.
3. Enter a user name for the Administrator account.
4. Select Administrator from the **Administrator** Role list.
5. Enter and confirm (re-enter) a password for the new user.
6. Click **Finish**.

To edit an Administrator account:

1. Go to **Setup > Access Control**.
2. Next to the account name, click **Edit**.
3. Edit the settings as required.
4. Click **Save**.

To delete an Administrator account:

1. Go to **Setup > Access Control**.


Copyright © 2011, Juniper Networks, Inc.

2. Next to the account name, click **Delete**.

There is no undo option when deleting an account. Be sure you have the correct account before deleting it.

## Creating and Managing Provisioning User Accounts

Provisioning User accounts are created by Administrators. Provisioning Users are given explicit access to User Types. An Administrator can allow a Provisioning User to create and manage all or only a limited number of User Types.

A Provisioning User must be created with access to at least one User Type.

To create a Provisioning User:

1. Go to **Setup > Access Control**.
2. Click **Add**.
3. Enter a user name for the **Provisioning User**.
4. Select a Provisioning User from the Role list.
5. Enter and confirm (re-enter) a password for the new user.
6. Click **Continue**.
7. Assign the User Type by moving the appropriate User Types from the Available User Types to the Selected User Types to allow access to each.
8. Click **Finish**.

To edit Provisioning User:

1. Go t**o Setup > Access Control**.
2. Next to the account name, click **Edit**.
3. Edit the settings as required.
4. Click **Save**.

To delete a Provisioning User:

1. Go to **Setup > Access Control**.
2. Next to the account name, click **Delete**.

There is no undo option when deleting an account. Be sure you have the correct account before deleting it.

## Configuring Self-Signed Access Control

Configuring Self-Signed Access Control allows an Administrator to log into SmartPass and create and manage user accounts that allow specified access to the wireless network. This is useful when deploying a kiosk.

An Administrator user account must be created before a Self-Signed user account can be created. Once the Administrator account is saved, the Administrator can create many different types of user accounts and has the option to assign a Provisioning User to the account. To configure this feature, follow these steps:

1. Log into SmartPass and click **Setup**.

Copyright © 2011, Juniper Networks, Inc.

2. Click **Access Control** to display configuration options.
3. Under **Add Account**, click **Add**.
4. In the **Name** field, enter a name for the account.
5. From the **Role** list, select **Administrator**.
6. In the **Password** field, enter a password for the account.
7. To confirm the password, retype the password in the **Re-enter Password** field.
8. To save the account information, click **Finish**. You are returned to the Access Control page.

To configure a Self-Signed User, follow these steps:

1. Under **Local Accounts**, click **Add**.
2. In the **Name** field, enter a name for the account.
3. From the **Role** list, select **Self-Signed User**.
4. In the **Password** field, enter a password for the account.
5. To confirm the password, retype the password in the **Re-enter Password** field and click **Next**.
6. Under **Available User Types**, select the type of account that is needed for the Self-signed user and use the arrow options to move the **Available User Types** to the **Selected User Types** column and click **Next**.
7. Select a name from the **Available User Types** column and use the arrow options to move the **Available User Types** to the **Selected User Types** column and click **Next.**
8. Under **Available Provisioning Users**, select the desired Provisioning User and use the arrow options to move it to the **Selected Provisioning Users** column and click **Finish**.

   If you have no **Available Provisioning Users**, click **Finish**.

## Assigning a Provisioning User to a Self-Signed User Account

Administrators have the option to assign a Provisioning User to an Self-Signed user account. The Provisioning User account must be created before it can be assigned to a Self-Signed User account. To configure a Provisioning User, follow these steps:

1. Under **Add Account**, click **Add**.
2. In the **Name** field, enter a name for the account.
3. From the **Role** list, select **Provisioning User.**
4. In the **Password** field, enter a password for the account.
5. To confirm the password, retype the password in the **Re-enter Password** field and click **Continue**.
6. Select a name from the **Available User Types** column and use the arrow options to move the selected **Available User Types** to the **Selected User Types** column and click **Finish.**
7. Click **Edit** next to the **Self-Signed User.**
8. Click **Edit** under the **Can be managed by the provisioning users** option.
9. **Selected Provisioning Users** is displayed. Use the arrow options to move the desired **Available Provisioning Users** to the **Selected Provisioning Users** and click **Save.**

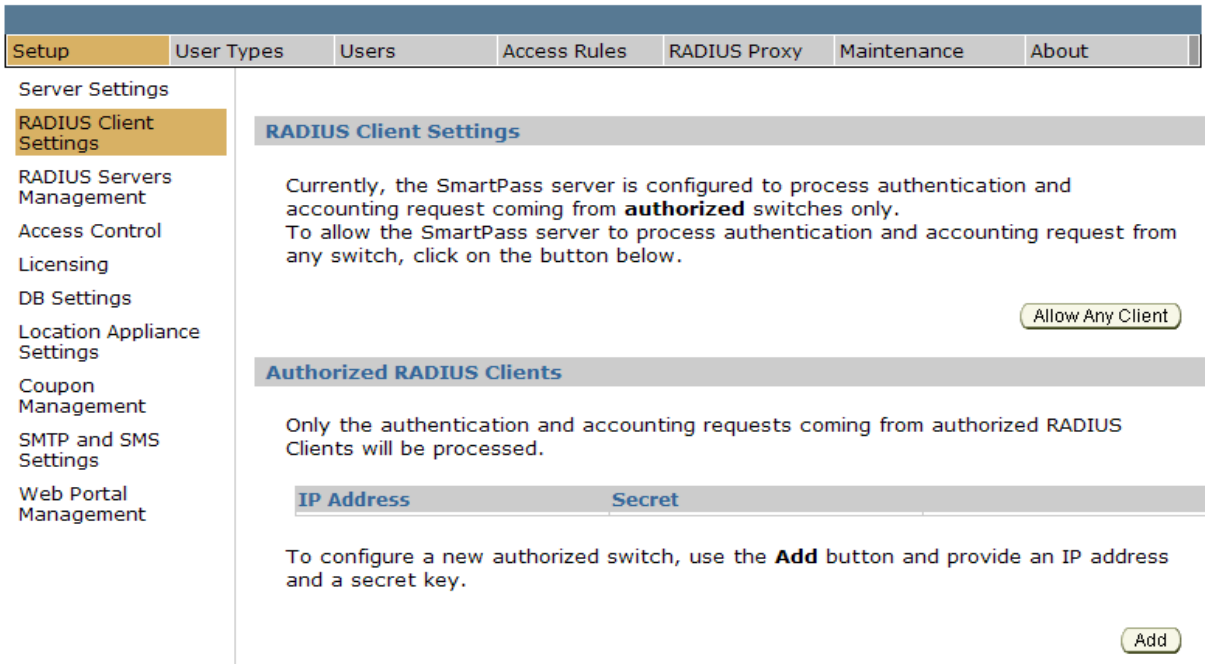
The selected Provisioning User is added to the **Can be managed by the provisioning users** option. Click **Save**.


Copyright © 2011, Juniper Networks, Inc.

# Adding an MX as a RADIUS Client on SmartPass

For SmartPass to be able to receive and send RADIUS messages to an MX, the MX must be configured as a RADIUS client on the SmartPass server. The SmartPass server and the MX must share the same secret key to be able to communicate. To add and MX as a RADIUS client, use the Add MX wizard.

1. Go to **Setup > RADIUS Client Settings**.
2. Click **Add.**


Setup
User Types
Users
Access Rules
RADIUS Proxy
Maintenance
About
Server Settings
RADIUS Client Settings
RADIUS Servers Management
Access Control
Licensing
DB Settings
Location Appliance Settings
Coupon Management
SMTP and SMS Settings
Web Portal Management
RADIUS Client Settings
Currently, the SmartPass server is configured to process authentication and accounting request coming from authorized switches only.
To allow the SmartPass server to process authentication and accounting request from any switch, click on the button below.
Allow Any Client
Authorized RADIUS Clients
Only the authentication and accounting requests coming from authorized RADIUS Clients will be processed.
IP Address
Secret
To configure a new authorized switch, use the Add button and provide an IP address and a secret key.
Add

3. Enter the **IP Address** and **Shared Secret** of new MX.
4. Click **Save**.

## Using the Allow any Client Option

SmartPass can be configured to exchange RADIUS messages with an MX with the correct shared secret without regard to the IP addresses of the switch.

1. Go to **Setup > RADIUS Client Settings**.
2. Click **Allow Any Client**.
3. Click **Edit**.
4. Enter the **Shared Secret** and click **Save**.

Now that SmartPass is in the “Allow Any RADIUS Client mode” the SmartPass server collects data about specific NAS IPs through successful accounting message exchanges and successful dynamic authorization message exchanges. These switches are added to a list called Learned RADIUS clients list. The user can change Learned RADIUS client to configured RADIUS clients.

# Database (DB) Settings

This is a timer feature used to purge the SmartPass Guest database of all expired Guest accounts. Guest accounts that expired but have not been purged from the database can be reactivated by any Administrator or by the appointed Provisioning User for the Guest Account.

Copyright © 2011, Juniper Networks, Inc.

To purge expired Users:

1. Login as an Administrator.
2. Go to **Setup > DB Settings**.
3. Enter the amount of time in hours that SmartPass waits before purging expired users.
4. Click **Save**. The purge action is not automatically scheduled. In order to delete the data you need to click **Save** and confirm the purge action after being informed about the consequences. If expired users are successfully purged, a “Delete expired users task was successfully restarted” message is displayed.
5. You can also enter the amount of time in days that SmartPass waits before deleting expired data. Click **Delete Now**. You must confirm that you want to delete the monitoring data. Data deletion does not affect the server operation in progress. The server is not restarted.


Copyright © 2011, Juniper Networks, Inc.

# Location Appliance Settings

One of the main features of SmartPass is the integration of SmartPass Services with the LA-200. By integrating with the LA-200, SmartPass has been given access to the real-time location of each client in the network. SmartPass Services can query one or many LA-200s to obtain the locale information of clients and uses the locale information to either deny or authorize clients or change client authentication attributes as clients roam on the network.

## Location Appliance Settings

1. Add a Location Appliance by typing in a specific **IP Address**, **Port**, **User Name** and **Password** and click **Add**. The Location Appliance is displayed in the Location Appliance Server List.
2. You have the option to enable the Location Appliance Poll and enter a time (in seconds) to determine how frequently SmartPass polls the network for user information.
3. Under Location Appliance Security Settings / Connection Security you can select from the following options:
   - Accept All Certificates
   - Accept Self-Signed Certificates
   - You can also upload a certificate into the **Certificate Trust Store** by typing in **File** name, **Type** and **Password** and clicking **Save**.

### Refresh Locale List

Under the **Location Appliance Server List** is a list of Location Appliance Servers, IP Addresses, Port numbers and User Names. You can manage servers by clicking on **Edit** or **Delete** to delete the server.

Clicking **Refresh Locale List** causes SmartPass to query the relevant LA-200 Appliance and retrieve the list of locales. The updated information is displayed when configuring the Access Rules and is also used to trigger them. The updated information is also stored as accounting information from the LA-200 Appliance.

# Coupon Management

## Coupon Enhancements in SmartPass 7.6

New print, e-mail, and SMS options are available for SmartPass 7.6 coupons. The SP-GA-xx license is required for coupon printing. The SP-SM-xx license is required for e-mailing and SMS options.

- You can print coupons in HTML. Printing coupon in PDF is optional.
- You can e-mail coupons with custom tags (SSID name, Username, Password, User-Type, Start and End Date).
- You can e-mail (secure SMTP) the authentication information/coupon to the User.
- You can send an SMS with the authentication information (Username/ password, start and end time and date) per User type.
- Additional fields are available when you create an account for e-mail, phone number, SMS, and company name.

## Coupon Management

Coupons can now be managed in the **Setup > Coupon Management > General Preferences** section. You can create Custom and Built-in coupons and configure E-mail and SMS template placeholder settings for your coupons.

Copyright © 2011, Juniper Networks, Inc.

You can use placeholders for both E-mail and SMS templates. When the coupons are e-mailed or sent by text message, each placeholder is replaced with the proper value for each User. You can view a list of all valid placeholders by clicking the **See supported placeholders** link, as shown below.

The available E-mail and SMS settings that can be configured are described in the table below.

| Setting Name | Component Type | Default Value | Description |
|---|---|---|---|
| Subject | Input Text | Login details for wireless network NETWORK_NAME | Configure the subject of the e-mail sent to the Users. |
| Include Attachment (PDF) | Check box | Checked | Configure if you want to attach a PDF version of the coupon to the e-mail.<br><br>This option is taken into account only for built-in coupons. |
| Message Template (E-mail section) | Input Text, Multi-line | Dear PERSON_NAME, Please find below the details for accessing the wireless network NETWORK_NAME. THE_COUPON Yours, | Configure the content of the message sent by e-mail to the Users. The THE_COUPON placeholder is be replaced by the actual HTML coupon. |
| Save (E-mail section) | Button | N/A | Save the E-mail settings in the configuration file |
| Message Template (SMS Section) | Input Text, Multi-line | User credentials for NETWORK_NAME: Username: User_NAME; Password: User_PASSWORD; Valid from VALID_SINCE to EXPIRATION_DATE. | Configure the SMS text which is be sent to Users. |
| Save (SMS Section) | Button | N/A | Save the SMS settings in the configuration file. |

### Coupon Template Management

The Coupon Template Management section has a table that displays both Custom and Built-in configured coupons. You can use Edit, Preview, and Delete options for each coupon entry.

The **Preview as PDF** action becomes available only if the coupon is a built-in type. **Preview as PDF** action opens a PDF file of the sample coupon in a new page of the browser.

## SMTP and SMS Settings

New menu items **SMTP** and **SMS Settings** have been added under the **Setup** menu. An Administrator must set up the SMTP and Text Message Profiles before sending coupons by e-mail and/or text message.

### SMTP

The SMTP section has an **Add** option and a table of the existing SMTP Profiles. Click **Add** to open the **Add SMTP Profile** wizard, which is shown below.

Passwords for the SMTP Profile are encrypted before being saved in the database.

A Default profile always exists and is the default SMTP association for each User-type. The Default SMTP profile cannot be deleted.


Copyright © 2011, Juniper Networks, Inc.

All SMTP profiles are listed in a management table. An Administrator can **Edit**, **Send Test E-mail**, and **Delete** options for each SMTP profile.

The **Edit** option for the Default profile allows you to leave the Server Hostname field empty and to skip validation. A Default configuration with missing elements cannot be used for sending e-mails.

The **Delete** action works with existing User-types associations. If a SMTP Profile is already associated to one or more User-types, then you cannot delete the profile. The Administrator is required to remove the associations first.

If you want to test a SMTP profile e-mail setup, select **Send Test E-mail.** A **Test SMTP Configuration** pop-up page like the one shown below displays. You can send a test e-mail using the associated profile.

If the test e-mail cannot be sent, an error message displays.

## SMS

SmartPass 7.6 relies on Clickatell, a SMS Gateway, and the Mail2SMS feature provided by the mobile phone carriers to send a text message from a web application. The SMS section has an **Add** button and a table of the existing profiles. You can create one or more SMS Profiles based on either Clickatell or E-mail To SMS.

Clicking the **Add** button opens a two-page wizard. On the first page you select a profile based on Clickatell or the E-mail to SMS technology using a dropdown box.

If the **Clickatell** profile is chosen and you click **Next**, you are taken to the A**dd Clickatell SMS Profile**. Type in your Clickatell SMS Profile information.

All the fields of the **Add Clickatell SMS Profile** form are required. The authentication details (API ID, Username and Password) are obtained when creating a Clickatell Central account on the www.clickatell.com website. The API ID must be the one corresponding to the XML API offered by Clickatell.

If the **Email To SMS profile** is selected from the **Add SMS Profile** wizard page, the following page is shown.

A profile name is required and a list of Email to SMS Gateways must be compiled to be associated with the profile. At least one gateway is required.

Both the Clickatell profiles and Email to SMS profiles are shown in the same table, under the SMS Settings section, as shown below.

Each configured SMS Profiles have three associated actions: **Edit**, **Delete** and **Send Test SMS**.

The **Edit** action starts the **Edit Clickatell Profile wizard** or the **Edit Email to SMS Profile wizard**.

The **Delete** action checks to see if the selected profile is currently associated to any User-type. If no association is found, it is deleted. If an association is found, the profile is not deleted and an information message displaying the list of associated User-types is displayed.

The **Send Test SMS** action opens a pop-up page that you can use to send a test SMS with the associated profile. If the test SMS fails, an error message appears.

A Default SMS Profile always exists in the **SMS Profiles** table and is the default association for each User-type. This Default profile cannot be deleted. The settings of this Default profile are listed below:

- Profile Name: Default
- SMS Profile Type: Clickatell
- API_ID: blank
- User: blank
- Password: blank

Copyright © 2011, Juniper Networks, Inc.

In the SMS Profiles table, there is an **Update Email to SMS Gateways** link that allows the modification of the gateway's database. Click the link to open the table of existing **Email to SMS Gateways**, like the one shown below.

By default, this table is prepopulated with a list of known gateways, based on the information found at http://www.mutube.com/projects/open-email-to-sms/gateway-list/. You can delete an entry or add a new gateway by providing the country, carrier name and e-mail address format. Click **Add** to automatically update the table.

The **Email to SMS Gateway** also contains an **In Use** column, which tracks associations between gateways and profiles. If the value of the **In Use** column of an entry is **Yes**, then the entry can not be deleted and the **Delete** button is disabled.

## User-Type Configuration Changes

You have the option of sending the coupon to a User by Email and/or SMS is enabled per User-type. This means that when you create or edit a User-type, you can select a SMTP or SMS profile that is used to e-mail the associated Users with their authentication details and instructions.

The **Create/Edit User-Type** wizard has a new optional page (in the Create User Type Wizard) that is used for configuring E-mail and Text Message Settings.

## User Configuration Changes

The Create/Edit User form also has a new **Contact Details** section:

The default SMS profile is used if the User Type associated to a User is configured to use an E-mail-to-SMS profile but no carrier is selected.

The Name field has been renamed to **Account Name**, in order to differentiate between the two name fields: Account Name and Person Name.

## E-mail/Text Message Related Actions

The following new actions have been added to the drop-down global **Actions** menu in the **Users > Users Management** table to accommodate the new E-mail/Text Message options:

- **Save Coupons**
- E-mail Coupons
- **Text Coupons**

The following new actions have been added to the drop-down Per-User **Actions** menu to accommodate the new E-mail/Text Message options:

- Save Coupon
- E-mail Coupon
- Text Coupon

The Print Coupon action has been renamed **View and Print Coupon**.

## Global Save Coupons Action

The global **Save Coupon** action opens a new page, which allows you to select one of the following save modes:

- **PDF File** - each User coupon is saved on a separate page of the PDF file
- **Zip Archive** - each User coupon is saved in its own PDF file


Copyright © 2011, Juniper Networks, Inc.

Also, a table containing all the Users with coupons that can be converted to PDF are shown. A coupon can be converted to PDF only if it is a built-in coupon.

After selecting the save mode, click **Save Coupons**, which starts the download.

If the **PDF File** option is chosen, the User is prompted to download a PDF file. Each page of this file represents a User coupon.

If the **Zip Archive** option is chosen, the User is asked to download a .zip archive containing a PDF file for each User coupon.

### Per User Save Coupon Action

The per-User **Save Coupons** action starts the download of the PDF file. If the coupon of the selected User cannot be converted to PDF, an error message displays at the top of the main page.

### Global E-mail Coupons Action

The global **E-mail Coupons** action redirects the User to a new page with a table that contains the subset of selected Users to which an e-mail can or cannot be sent.

### Per User E-mail/Text Coupon Action

If an e-mail or text cannot be sent to a user based on the configuration requirements, an error message is displayed which lists the reason why the coupon cannot be e-mailed.

If the e-mail or text is successfully sent the user is informed of the result.

### Global Text Coupons Action

The global Text Coupons action redirects the user to a new page with a table that contains the subset of selected Users to which a Text Message (SMS) can or cannot be sent. A SMS can be sent to a user if you have the following:

- A mobile phone number is defined for the user
- A Send Coupon by SMS is enabled for the associated user-type
- The associated SMS profile per user-type is an E-mail to SMS Profile, and a carrier is chosen at the user level
- The associated SMS profile is a fully configured Default profile

Each correctly configured user in the table has an available preview of the text message, number of characters used, and the number of message to be sent.

You also havethe option of sending the text message (**Send Text Messages**) or canceling it (**Cancel**).

If the action is cancelled, you are redirected to the main Users page.

If the **Send Text Messages** button is clicked, SmartPass attempts to send all the text messages. You are redirected to a **Send Text Messages Results** page, where there is a list of sent SMS messages, failed messages, and the reasons for failures.

### Create User

The **Users > Create User** wizard has two new Action options: **E-mail Coupon** and **Text Coupon**.

**E-Mail Coupon** is enabled only if the associated user-type has the **Send Coupons by E-mail** setting enabled and the e-mail field is configured.

**Text Coupon** is enabled only if the associated user-type has the **Send Coupons by SMS setting** enabled and the Mobile Phone Number is configured.

If the E-mail/SMS cannot be sent, an error message is shown on the top of the **Create User** page. If the E-mail/SMS send coupon action is successful, a confirmation message is displayed.

### Bulk Create Users

The **Users > Bulk Create Users** page allows you to create Users with the following actions:

Copyright © 2011, Juniper Networks, Inc.

- Specifying user names mode
- Generating user names
- Importing Users from CSV

If one of the first two methods is used, there is no way to associate an E-mail Address or Mobile Phone Number to each user at the time the User is created. If you want to configure these fields, you need to edit each one of User profile and provide valid E-mail Address/Phone number.

The Import Users from CSV mode has been improved. The imported CSV file contains the following new columns:

- EMAIL_ADDRESS
- PHONE_NUMBER
- PERSON_NAME
- COMPANY_NAME

If the imported CSV File contained the EMAIL_ADDRESS column, **E-mail Coupons** is displayed on the top of the Import Results table after creation.

If the imported CSV File contained the PHONE_NUMBER column, **Text Coupons** is displayed on the top of the Import Results table.

Earlier versions of SmartPass used to verify usernames while importing a CVS files if the username already existed. If the user name did exist, the system would not add it again and skip past it. Now in that SmartPass 7.6 prompts the User to update the existing user information. If you **Skip existing users**, the old behavior is kept. If you select **Override existing users**, the user information is updated.

## Logging

Each time a coupon is e-mailed or sent as SMS to a user/group of users, the event is logged under a new **Coupons** module.

## Licensing

The PDF coupons capability is available with any license. SMS and E-mail notification options require the Subscriber Management license.


Copyright © 2011, Juniper Networks, Inc.

# Web Portal Management

## Web Portal Authentication Server

The new Web Portal Authentication Server features are available with the SP-SM-xx license and rely on the External Captive Portal feature introduced in Mobility System Software (MSS) Version 7.0. The new features allow an Administrator to offload the hosting of Web portal pages from the MX and authenticate Web login users against an external RADIUS server or SmartPass local user database service.

In this case, Web users are authenticated as follows:

1. Users connect to a Web portal-enabled service.
2. All user traffic is blocked except DNS requests.
3. HTTP data is redirected to a configured external authentication Web server (SmartPass). This occurs when you configure a dedicated Access Control List (ACL) and set the "web-portal-form" attribute to the Web portal service profile.
4. The SmartPass server interacts directly with the User's web browser to validate credentials.
5. Once credentials have been confirmed, SmartPass sends a CoA request, which contains a request for a session username change to the originating MX. The Web portal session becomes authorized and active at the same time. The Web portal ACL is then removed to allow normal traffic over the network. Additional CoA attributes are set by the external Web server at the same time.

This 7.6 SmartPass feature only works in conjunction with MXs running MSS 7.0 or later. SmartPass allows Users to authenticate locally on the SmartPass database or via an external RADIUS server (configured as a RADIUS proxy). Also, SmartPass needs to be setup as a DAC to the MX.

## Web Portal Management Page

Web Portal Management is now available as part of the SmartPass Setup menu to accommodate the Web Portal Authentication Server feature. As an Administrator, you can use this feature to assign an authentication page to a specific SSID. There is also a table that displays the following:

- SSID Name
- Web Authentication Type
- Active status
- Page set type

You can add Web Portals to SmartPass by clicking **Add Web Portal Configuration.** You are redirected to a **Create Web Portal Configuration Wizard**.

After you add the Web Portal configurations to SmartPass, each SSID name has an **Actions** menu that allows you to **Activate/Deactivate**, **Edit**, **Preview**, **Login**, **Redirect**, **Preview Logout** and **Delete the Web Portal Authentication configuration**.

Copyright © 2011, Juniper Networks, Inc.

# Web Portal Configuration Wizard

## Deleting SSID Configurations

You can use the **Delete** action item in the management table to remove the SSID to Web Portal Configuration association from the configuration file. You must confirm the action by clicking yes on the message “Are you sure you want to delete the <SSID_NAME> Web Portal configuration?”

A Default SSID configuration cannot be deleted.

## Adding SSID Configurations

1. Go to **Setup > DB Settings**.
2. Click **Add Web Portal Configuration**. The first page of the Create a new Web Portal Configuration wizard opens.
3. Type in a SSID Name and click the Upload Custom HTML files box if you want to use a custom HTML file for the web portal.
4. Click **Next** to go to Step 2 of 5. **Finish** returns you to the **Setup > Web Portal Management** page where your new Web Portal Configuration is saved. Default settings are used for all remaining Web Portal options.
5. On Step 2 of 5 select either **Local** or **External** as your Authentication Type. If you select Local, you have the option of using cookies and selecting a **Cookie lifetime** by filling in the box. If you select **External** Authentication Type then you have the option to **Use the Local server as a failover server** by checking the available box.
6. Click **Finish** to return to the **Setup > Web Portal Management** page or **Next** to go to Step 3 of 5.
7. On Step 3 of 5 you have the option to customize your log-in page image and script. Default wording and a Juniper Networks image are supplied. Make any edits and click **Next**, **Preview** or **Finish**.
   - **Next** takes you to Step 4 of 5 Logout Page customization where you have the option to customize your log-out page image and script. Default wording and a Juniper Networks image are supplied.
   - **Preview** lets you preview your Login page. Click **Close** to return to Step 3.
   - **Finish** returns you to the **Setup > Web Portal Management** page where your Web Portal Configuration is saved. Default settings are used for the Web Portal Logout.
8. Click **Next** to go to Step 4 of 5 b**uilt-in Logout Page customization - Default SSID**.
9. Decide whether to **Enable logout** on your customized Logout page and customize your logout page image and script. Default wording and a Juniper Networks image are supplied. Make any edits and click **Next**, **Preview**, **Finish** or **Cancel**.
10. Click **Next** to go to Step 5 of 5 **Redirect Page Customization - Default SSID**.
11. Select **Enable redirect** and your desired Refresh Time on your customized Redirect Page and customize your image and script. Default wording and a Juniper Networks image are supplied. Make any edits and click **Preview**, **Finish** or **Cancel.**
12. Click **Finish** to save the Web Portal Configuration. The **Setup > Web Portal Management** page is displayed where your Web Portal Configuration is saved. You can use the **Action** drop drown options to **Deactivate**, **Edit**, **Preview Pages**, and **Delete** your Web Portal Configuration. The default Web Portal Configuration cannot be deleted.


Copyright © 2011, Juniper Networks, Inc.

## Configuring SmartPass as an External Captive Portal Server

To configure SmartPass as an external captive portal server please refer to the *Juniper Networks Mobility System Software Configuration Guid*e.

The redirect URL should be configured as https://<SP_SERVER_ADDRESS>/gp2/webportal/ext/webPortalAuthLogin.

We also ship samples with the product in case configuration screenshots are needed.

# Configuring the SmartPass Connection to the MX

This section describes SmartPass communications with one or more MX devices. It also describes the procedure(s) for configuring the MX to support SmartPass and Users.

You need the IP Address of the MX device(s) to connect, and the shared secret for each.

Shared secrets may be of any length (except 0 length). For strong security that is virtually impossible to break by any brute force method, a shared secret should be at least 16 characters in length and contain a combination of letters, numbers, and special characters.

It is not necessary to pre-configure the MX before configuring SmartPass to connect to it. However, you must configure the MX before the connection is established.

# Configuring the MX to Support SmartPass

There are two ways to configure the MX:

- RingMaster
- CLI

You need the following information for the configuration of the MX:

- IP address of the SmartPass Server as the RADIUS server for authentication and accounting as well as the Dynamic Authorization Client (DAC).
- The shared secret must be the same for all SmartPass configurable functions.

The SmartPass server should have a static IP address. If the server is configured to receive an IP address from a DHCP server, you cannot to connect to the MX if the DHCP lease renews with a different IP address.

# Adding SmartPass Server as a RADIUS Server on the MX (CLI)

1. Create a Web Authentication service with the SmartPass server as the authenticating RADIUS server.

```
set service-profile name ssid-name ssid-name
set service-profile name ssid-type {clear | crypto}
set service-profile name auth-fallthru {web-portal | none | last-resort}
set service-profile name auth-dot1x [disable | enable]
set service-profile name web-portal-acl portalacl
set service-profile name attr vlan-name vlan-name

set radius server smartpass address 172.21.16.233 timeout 30 retransmit 3 dead-
        time 0 key smartpass
```

Copyright © 2011, Juniper Networks, Inc.

```
set server group smartpass-group members smartpass
set authentication web ssid smartpass ** smartpass-group
```

2. Associate the SmartPass server as the accounting server for the relevant SSIDs. Depending on the type of authentication mechanisms used for the various SSIDs, one or more of the following commands may need to be entered.

Any SSIDs not on the list do not report accounting data to the SmartPass server and cannot be used to trigger Access Rules.

```
set accounting system smartpass-group
set accounting web ssid smartpass ** start-stop smartpass-group
```

-or-

```
set accounting web ssid any ** start-stop smartpass-group
```

-or-

```
set accounting last-resort ssid any start-stop smartpass-group
```

-or-

```
set accounting dot1x ssid any ** start-stop smartpass-group
```

3. Set the SmartPass server as the DAC for all SSIDs.

```
set authorization dynamic ssid any smartpass
set radius dac smartpass address 172.21.16.233 replay-protect disable key test
```

# Configuring the MX With RingMaster

**RingMaster** (versions 6.2 and higher) allows you to configure **SmartPass** as an accounting and DAC server and also generate client session reports based on accounting information collected by the *SmartPass* server. There are two new wizards for setting **SmartPass** — one under the network plan and the other at the Radius level.

## SmartPass Network Level Setup

This wizard provides a single page with all the settings *RingMaster* needs to connect to *SmartPass* and query the accounting information for reports. These settings are used by other wizards to configure *SmartPass* as a RADIUS Server and RADIUS DAC. Only one *SmartPass* server can be configured for all MXs in a network plan.

1. Select **Configuration** in the Navigation Bar.
2. Select the Network Plan and select **SmartPass Server** in the **Tasks** panel.

   Enter the **Server IP Address**, **Port Number**, **Secret Key**, **User Name** and **Password** for the *SmartPass* server and click **OK**.

## SmartPass Wizard

This wizard helps you configure MXs to create a new service profile and use *SmartPass* as a RADIUS server.

There are three ways to access the **SmartPass** wizard:

a. In the **Organizer** panel, click the plus sign by an **MX** that is *not* in a cluster**.**
b. Click on **Wireless**.
c. Click on **Wireless Services**.
d. In the **Tasks** panel, select **SmartPass**.


Copyright © 2011, Juniper Networks, Inc.

**OR**

a. In the **Organizer** panel, click on **Cluster Configuration.**

b. Click on **Wireless Services**.

c. In the **Tasks** panel, select **SmartPass**.

**OR**

a. In the **Organizer** panel, click on the plus sign next to an MX.

b. Click on the plus sign next to **AAA**.

c. Select **RADIUS**.

d. In the **Tasks** panel, select **SmartPass**.

3. Click **Next**.
4. Fill in the dialog below by selecting an **IP Address**, **Port Number**, **Secret Key**, **User Name** and **Password** for *SmartPass*, then click **Next**.
5. You now see the **SmartPass Options** are displayed and you can select SmartPass RADIUS options to apply to the SmartPass server. Click **Next**.
6. Select an existing Service Profile or select **Create New Service Profile**, then click **Next**.
7. The SSID dialog appears:

   a. Select an **Access Type**.

   b. Enter a **Name** for the Service Profile.

   c. Select an **SSID Type**.

   d. Click **Next**.
8. You now see the **Wireless Security** dialog:

   Select desired security standards and then click **Next**.
9. You now see the **Wireless Security** dialog:
10. You now see the **Optional: Default VLAN** dialog:

    Select or enter a **VLAN Name**. Click **Next**.
11. You now see the **Radio Profile Selection** dialog. Select an existing profile and skip to step 14, or check **Create new  Radio Profile** and click **Next**.
12. If you selected **Create a New Radio Profile**, enter a **Name** and click **Next**.
13. You now see a table of **Available Members** APs that you can move to **Current Members** of the Radio Profile.

    Click **Finish**.
14. You select VLAN 802.11n Attributes to add to the profile.

    Select from the following:

    - **802.11ng Mode** — **Enable**, **Disable** or **Required**
    - **802.11na Mode** — **Enable**, **Disable** or **Required**
    - **802.11 Settings** — **Maximize Throughput** or **Maximize Compatibility**

The Guard Interval attribute defaults to the value Long.

## SmartPass Accounting Summary

To generate a **SmartPass Accounting Summary** report in RingMaster:

1. Select the **Reports** Navigation Bar button.
2. From the **Report Types** list, select **SmartPass Accounting Summary**.
3. To view an existing report, click on its name and select **View** in the **Tasks** panel.

Copyright © 2011, Juniper Networks, Inc.

4. To generate a new report, click **Generate**.
   Select parameters for the report from the **Report Options** list:
   - **Report Scope Type**
     - **Network Plan**
     - **Mobility Domain**
     - **Mobility Exchange**
   - **Report Scope Instance**
   - **Report Time Period**

   Add a Report Filter if desired.
5. Click **Next**. The report is generated.

## SmartPass Accounting Details

To generate a **SmartPass Accounting Details** report:

1. Select the **Reports** Navigation Bar button.
2. From the **Report Types** list, select **SmartPass Accounting Details.**
3. To view an existing report, click on its name and select **View** in the **Tasks** panel.
4. To generate a new report, click **Generate**.
5. Select parameters for the report from the **Report Options** list:
   - **Report Scope Type**
     - **Network Plan**
     - **Mobility Domain**
     - **Mobility Exchange**
   - **Report Scope Instance**
   - **Report Time Period**

   Add a Report Filter if desired.

Click **Next**. The report is generated.

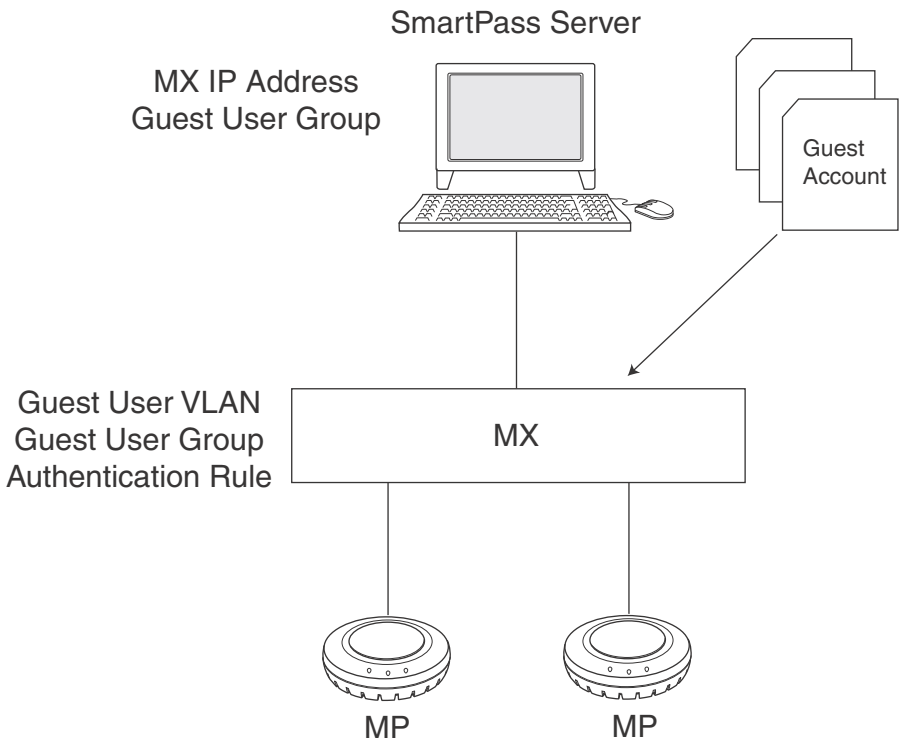

Copyright © 2011, Juniper Networks, Inc.

# SmartPass Guest Access

SmartPass is an application that enables non-IT staff to configure temporary user accounts for Guest access to your network.

With SmartPass and your MX you can control when and where your Guests have access to your wireless network. Creating multiple User Types with access restrictions and assigning User Types to specific VLANs allows you to maintain strict security and give you total access control over Guest wireless devices.

SmartPass integrates seamlessly into your existing Juniper Networks wireless network, as shown below.




## MX Configuration

Configuring an MX for SmartPass is performed by the network Administrator to allow only the user groups or VLANs accessible by Guest wireless users.

## User Groups

A user group assigns users to a VLAN and optionally can set other attributes as well. The MX must have a user group so that SmartPass uses the MX for Guest Access. Juniper Networks recommends that you create a separate user group used only for Guest Access.

Copyright © 2011, Juniper Networks, Inc.

One of the attributes you can configure for a user group is end-date. However, SmartPass sets this attribute automatically based on information entered by the Guest access Administrator when creating the Guest account.

The bonded option uses Bonded Auth™, which requires a user's computer to successfully complete authentication before the user can be authenticated. Use this option only if you plan to configure a separate authentication rule for computers on the network.

### Fallthru Authentication

If a User matches the userglob in an 802.1X authentication rule, but the network interface card (NIC) for the user does not support 802.1X, the MX attempts to authenticate the user with the fallthru authentication type, which is WebAAA by default for wireless access. (The default fallthru authentication type for access through a wired authentication port is none, which means the user is denied access.)

To allow users with NICs that do not support 802.1X for network access, configure a WebAAA authentication rule in addition to an 802.1X rule. For example, the following rules attempt 802.1X authentication for all usernames that begin with *Guest*, but use WebAAA authentication for any User whose NIC does not support 802.1X:

```
set authentication dot1x ssid guest-ssid guest* peap-mschapv2 local
set authentication web ssid guest-ssid guest* local
```

The first rule attempts to use PEAP-MSCHAP-V2 to authenticate the User. If the user does not support 802.1X, the second rule uses WebAAA.

## Creating and Managing Users

This section discusses the interface and controls for creating and managing users. Examples of how to perform the various procedures follow each major section.

## Creating Custom User Types

Use the Create User Wizard to create Custom User Type profiles and to set restrictions per user.

1. Login as an Administrator.
2. Go to **User Types > Create User Type**.
   a. Enter a **User Type Name**. After the User Type profile is saved, this User Type name appears in the list of Custom User Types found in **User Types > User Types Management**.

The specified name must be at least 1 character in length and be no more than 25 characters in length. The name may contain Alpha-numeric characters (A-Z,A-z, 0-1) and special characters such as $, %, and *.

   b. Enter a **VLAN Name** of the VLAN used to route user traffic. Use **default** to specify the default VLAN configured on the MX for SmartPass users. You may specify a different VLAN if you want to place your User Type on a VLAN other than the default VLAN.
   c. Select the **Allow per-user end date** option to specify a user's end date.
   d. Enter general information about the User Type in the **Description** field.
3. Select **Next** to continue adding restrictions to the User Type or **Finish** to save the User Type name and exit the wizard.
4. If **Next** is selected,**Restriction Access** options are displayed.
   a. Select the **Restricted to a MAC address** option to configure MAC address restrictions per User Type. This prevents simultaneous logins using a single user profile because the user is


Copyright © 2011, Juniper Networks, Inc.

restricteded to the MAC address that they successfully log in with for the first time. All users configured as this User Type are now restricted by MAC address on the network.

**b.** Select the **Password Management** option to set a maximum number of unsuccessful authorization attempts that can be made by a user within a specific time when logging onto the wireless network. When the **Password Management** option is selected, the **Time Interval** and **Number of Retries** fields become available.

**c.** In the **Time Interval** field, enter a value between 1 – 86400 seconds. The default value is 60 seconds.

**d.** In the **Number of Retries** field, enter a value between 1 – 100. The default value is 3.

**e.** Select the **Lock on Disconnect** option to prevent users from reconnecting after they are disconnected by an Administrator using the **Disconnect** action on the **Users > Users Management** page.

**5.** Select **Next** to continue adding restrictions to the User Type or **Finish** to save the User Type restrictions and exit the wizard.

**6.** Click **Next** and the **Time Restrictions** options are displayed. You can configure restrictions on the times, dates, and length of authorization for user access to the network.

**a.** Select the **Restrict access** option. When the **Restrict access** option is selected, the time and date restriction fields become available and the **Restrict duration (hours)** option is automatically selected as a default. Also, when the **Restrict Access** option is selected the **Finish** button becomes available because time restrictions must be set on the next page before saving the User Type profile.

---

When selecting more than one type of restriction it is important to remember that all the conditions for access must be true for the user to gain network access.

For example, if you select **Restrict duration (hours)** and **Select start and end date** options, then set the duration for 12 hours and an end date for a week later, the user's access expires 12 hours after activation and not at the end of the week period.

---

**7.** Select **Next**.

**a.** Enter a number in the **Duration (Hours : Minutes)** field.

**b.** Select the **Activate Immediately** option to allow user access beginning on the start date as opposed to beginning when the user authenticated within the selected dates.

**c.** Enter a **Start Date** and **End Date** or click the date selector icon to select a date.

**d.** Select a month and year from the pop-up calendar for the **Start Date** and **End Date**.

**e.** Your selections appear on the **Restriction Access** page.

**f.** You can also specify a time of day restriction for the User Type by selecting a **Time of Day** option. **Any** and **Daily** options have set hours, but the **Business Hours** selection has hour and minute drop-down options that can be set.

**g.** You can also click **Add Day** to allow the user access on an additional day during set hours.

**8.** Click **Finish** to save the User Type restrictions and exit the wizard or **Next** to go to the **Optional: Create User Type - Authorization Attributes** page.

**9.** Click **Next**.

**a.** Select options such as **Encryption Type**, **Mobility Profile**, and **Service Type** to set other VSAs (Vendor Specific Attributes) for User Type authorization. Definitions and further explanations of the VSAs are available in the *Mobility System Software Configuration Guide*.

**10.** Click **Next**.

Copyright © 2011, Juniper Networks, Inc.

11. The **Create/Edit User-Type** wizard has a new page that is used for configuring E-mail and Text Message Settings.You have the option to allow the sending of coupons to a User by Email and/or SMS that can be enabled per User-type. This means that when you create or edit a User-type, you can select a SMTP or SMS profile that is used to e-mail the associated Users with authentication details and instructions.
12. You have the ability to edit the MAC address restrictions that apply at authentication by selecting the **Edit MAC Address List** menu option of each User Type in the management table. If there are no MAC Addresses on the list, you can add or import allowed MAC Addresses and MAC Address pattern list by clicking **Add** or **Import** or click **Refresh** to update a populated list**.**
    a. For User-Type Bonded Authentication, SmartPass allows a provisioning user to specify any number of MAC Addresses by:
    - Importing a regular text file containing MAC Addresses patterns, one on each line
    - Copying and pasting a list of MAC Address patterns into a text area

    A MAC Address pattern allows a full or partial MAC Address to be specified, which ends in an asterisk wildcard (00:11:*).

    When you click submit, the specified list of MAC Address patterns are added to the existing list of Bonded Authentication MAC Addresses.
13. An **Add** or **Import MAC Addresses or MAC Patterns from a file** box appears after clicking **Add** or **Import**. Add your desired MAC addresses and other information and click **Save**. You are returned to the previous page..
14. Click **Finish**.

## Managing User Types

The **User Types Management** page allows Administrators and selected Provisioning Users to view the pre-defined and custom User Types and descriptions. Custom User Types can also be viewed, edited, or deleted here.

## Editing a Custom User Type

1. Go to **User Types > User Types Management**.
2. Next to a **User Type Name**, select **Edit** from the **Actions** list and click **Go**.
3. The **Create User Type** wizard is displayed. Go through the Wizard steps again, editing the information as necessary and click **Finish**. You can click **Finish** at anytime in the editing steps.

## Deleting a Custom User Type

1. Go to **User Types > User Types Management**.
2. Next to a **User Type Name**, select **Delete** from the **Actions** list and click **Go**.
3. Click **OK** to delete User Type or **Cancel**.

## Viewing a Custom User Type

1. Go to **User Types > User Types Management**.
2. Next to a **User Type Name**, select **View** from the **Actions** list and click **Go**. The selected User Type details are displayed.
3. Click **Return**.


Copyright © 2011, Juniper Networks, Inc.

# Creating and Managing Users

Users may be created and managed by either Administrators or Provisioning Users. In this section you create a User, edit and delete Users, and print User Coupons. Administrators can create Users and view and edit existing Users by using options under the **Users** tab.

When using SmartPass to manage your Users you can perform the following tasks:

- Create Users
- Create Batches of Users
- Delete Users
- Reactivate expired Users
- Change a User's password
- Change a User's User Type
- Disconnect a User
- Print a User Report.

A Provisioning User may only see the Users that the Administrator has given them permission to see.

A Provisioning User may only view, modify, and delete Users that were created from the account from which they were created. However, Administrators can see all Users.

**For example**: if a Provisioning User (Front Desk) creates a User (John_Doe), another Provisioning User (Accounting) cannot view or modify John_Doe.

## User Types

SmartPass was created with 6 pre-defined User Types that can be used to create specific User Types.

The pre-defined User Types include:

- **1-Hour Duration** — Permit access for one hour. The User account is activated upon the User's first successful authentication.
- **12-Hour Duration** — Permit access for 12 hours.
- **24-Hour Duration** — Permit access for 24 hours.
- **5-Days** — Permit access for 5 days.
- **5-Days Business Hours** — Permit access from every Monday to Friday between 8 AM and 5 PM but no more than 5 days.
- **Business Hours** — Permit access from every Monday to Friday between 8 AM and 5 PM.
- **Custom User Types** — Custom User Types accounts are also available for selection at the bottom of the User Type list. This means a custom User Type can also be used as a User Type.

## MAC and Bonded Authentication

The Create User wizard located under **Users > Create User** has three selections, which allows users to associate a User Name with a MAC Address for either of the following purposes:

1. Standard User - this option allows the SmartPass user to create a guest user that does not require any MAC Address related Authentication methods.
2. If a user selects MAC Address User, SmartPass only allows MAC Authentication for the specified MAC Address and if authentication is successful, it returns the user name as a User-Name Attribute in the RADIUS Accept message.

Copyright © 2011, Juniper Networks, Inc.

3. If a user selects MAC Address Bonded, SmartPass only authenticates this user if requests are coming from the specified MAC Address, i.e. the Calling-Station-ID RADIUS attribute matches the specified MAC Address. Rejected requests are logged with the appropriate reason.

   If MAC Address User or MAC Address Bonded User is selected then a valid MAC Address must be provided before the user can be created or modified respectively. You also have the option to fill in **Contact Details** for your User that is saved and accessed if you decide to configure E-mail or SMS options to send messages or coupons to your User.

## Creating Users

To create a User:

1. Go to **Users > Create User**.
   a. Enter a User name in the **Name** field.
   b. Select a **User Type** from the list.
   c. Enter and confirm a **Password** for your User
   d. Enter **Contact Details** for your User..
2. Click **Save**. A saved User account is activated when the user successfully authenticates for the first time.

If you want to create several new users, click **Clear** to clear information after saving your new User to clear the contents of the input fields and begin the process of creating another User.

## Creating Multiple Users at One Time

SmartPass gives you the ability to create many Users in one simple operation, by using the Bulk Create Users features.

You can create multiple Users in two ways:

- Specify names for each of the Users
- Allow SmartPass to generate them for you

  In either case, SmartPass generates random passwords for each new User.

### Creating Multiple Users

1. Go to **Users > Bulk Create Users**.
2. Click **Specify user names** option.
3. Select a **User Type**.
4. Enter the **User Names** for your new Users.

User names must be separated by either a comma or a space. User names must also be a single contiguous string of characters (e.g. JohnDoe or John_Doe).
If you have a long list of names you can save time by cutting and pasting the names from a comma or space delimited list of names.

5. Click **Generate**.

## Auto-generating User Names

1. Go to **Users > Bulk Create Users**.
2. Click **Generate user names** option.


Copyright © 2011, Juniper Networks, Inc.

3. Select a **User Type** from the list.
4. Enter a number in the **Number of Users** field.
5. Click **Generate**. A table of the new users is displayed.
6. Click **Print All** to print coupons which list User names, passwords and access instructions for each bulk saved Users or **Export to CSV File** to export the User information to a CSV file.

### Bulk Create MAC Address Users

The **Users > Bulk Create Users** page allows the bulk users to be created by:

- Specifying user names
- Generating user names
- Importing users from CSV file

If **Specify user names** or **Generate user names** options are configured, there is no way to associate an E-mail address or mobile phone number to each user at the time the User is created. If you want to configure these fields, you must edit user profiles and provide valid E-mail address/ phone number.

You can also select the desired MAC Authentication method for imported users. Select one:

- Standard User
- MAC Authentication
- Bonded MAC Authentication

The Import Users from CSV file has been improved in SmartPass 7.6. The imported CSV file contains the following new columns:

- EMAIL_ADDRESS
- PHONE_NUMBER
- PERSON_NAME
- COMPANY_NAME

If the imported CSV file contains the EMAIL_ADDRESS column, the **E-mail Coupons** button is displayed on the top of the Import Results table after creation.

If the imported CSV file contained the PHONE_NUMBER column, the **Text Coupons** button is displayed on the top of the Import Results table.

If there are existing users in the file, SmartPass prompts the user to overwrite the existing user information with new information. If you select **Skip existing users**, the old CSV file information is kept. If you select **Override existing users**, the user information is updated.

## Managing Users

You can use the **Actions** lists on the **Users > User Management** page to manage your list of Users.

### Showing User Details

To view **Guest Information**, **Last Login Time** and **MAC Address** of a User:

1. Go to **Users > User Management**.
2. Click **Show** next to a User on the list. The User information is displayed under the User column.

### Deleting Users

To delete a User:

1. Go to **Users > User Management**.

Copyright © 2011, Juniper Networks, Inc.

2. Select one or more User (s) from the list, select **Delete** from the **Actions** list and click **Go**.

## Disconnecting Users

To disconnect a User:

1. Go to **Users > User Management**.
2. Select one or more User (s) from the list.
3. Select **Disconnect** from the **Actions** list and click **Go**.

## Unlocking a User

To unlock a User:

1. Go to **Users > User Management.**
2. Select the **User Name**.
3. Select **Unlock** from the top **Actions** list and click **Go**.

## Clearing the MAC Restriction

To clear the MAC restriction option for a User:

1. Go to **Users > User Management.**
2. Select the **User Name**.
3. Select **Clear MAC Restriction** from the top **Actions** list and click **Go**.

## Printing a User Report

To print a User Report:

1. Go to **Users > User Management.**
2. Select the **User Name**.
3. Select **Report** from the top **Actions** list and click **Go**.
4. Click **Print** to print the report or **Return** to go back to the **User Management** screen.

## Exporting to CSV

To export a User Report:

1. Go to **Users > User Management.**
2. Select the **User Name**.
3. Select **Export to CSV file** from the top **Actions** list and click **Go**.
4. Open and view or save the Excel CSV file.

## Viewing and Printing Guest Coupons

SmartPass allows you to view and print a coupon with User names, password, and access instructions information to give to your User.

To print a coupon:

1. Go to **Users > User Management.**
2. Select **Print** from either of the **Actions** lists for the User and click **Go**.
3. You also have the option to print multiple user coupons at one time by selecting multiple Users then selecting **View and Print Coupons** from the **Action** drop down list. Each user coupon automatically prints on a separate sheet of paper.
4. Click **Print** or **Return**.


Copyright © 2011, Juniper Networks, Inc.

## Saving Coupons

To save coupons:

1. Go to **Users > User Management.**
2. Select one or more **User Names**.
3. Select **Save Coupons** from the **Actions** lists. This opens a new page that has a table that lists all the Users with coupons that can be converted to PDF. A coupon can be converted to PDF only if it is a built-in coupon. If the coupon of the selected User cannot be converted to PDF, an error message displays at the top of the main page.
4. Select a save mode and click **Save Coupons**, which starts the download.
   - PDF File - If the PDF File option is chosen, the User is prompted to download a PDF file. Each User coupon is saved on a separate page of a PDF file.
   - Zip Archive - If the Zip Archive option is chosen, you are prompted to to download a .zip archive containing a PDF file for each User coupon.

## E-mailing Coupons

To e-mail coupons:

1. Go to **Users > User Management.**
2. Select one or more **User Names**.
3. Select **E-mail Coupons** from the **Action** list. You are redirected to a new page with a table that lists the subset of selected Users to which an e-mail can or cannot be sent.
4. Click **Send E-mails** or **Cancel**.

If an e-mail cannot be sent to a user based on the configuration requirements, an error message is displayed which lists the reason why the coupon cannot be e-mailed.

## Texting Coupons

To text coupons:

1. Go to **Users > User Management.**
2. Select one or more **User Names**.
3. Select **Text Coupon** from the **Action** list. You are redirected to a new page with a table that lists the subset of selected Users to which a Text Message (SMS) can or cannot be sent. A SMS can be texted to a user if the following conditions apply:
   - A mobile phone number is defined for the user
   - A Send Coupon by SMS is enabled for the associated user-type
   - The associated SMS profile per user-type is an E-mail to SMS Profile, and a carrier is chosen at the user level
   - The associated SMS profile is a fully configured Default profile

   You can preview the text message, number of characters used, and the number of messages to be sent for each correctly configured user in the table by clicking **Show**under the Details column.
4. Click **Send Text Messages** or **Cancel.**
   - If you cancel the action, you are redirected to the main Users page.
   - If you **Send Text Messages** SmartPass attempts to send all the text messages. You are redirected to a **Send Text Messages Results** page, where you can view a list of sent SMS messages, failed messages, and the reasons for failures.

Copyright © 2011, Juniper Networks, Inc.

## Printing Single-User Coupons After Creating Users

Single-user coupons can be printed immediately after a new user is created using the wizard on the **Users > Create User** page after the **Print** button becomes enabled. In case a MAC user is created the USER_NAME placeholder value should be populated with the MAC user's associated MAC address. The option to print immediately after user creation is also valid for Provisioning or a Self-Signed users.

## Reactivating an Expired User

To reactivate an expired User:

1. Go to **Users > Expired Users**.
2. Click **Reactivate** next to the name of the User.
   A **Reactivate Expired User** page for the selected User is displayed.
3. Select a User Type, only if you want to change the User Type. Fill in the User's Contact Details (optional)
4. Click **Save**.

## Changing a Users Password

SmartPass allows you to change a User password.

To change a User password:

1. Go to **Users > User Management**.
2. Select **Edit** from the Actions list next to the name of the user and click **Go**.
3. Enter and confirm the new password on the **Edit User** page. Fill in the User's Contact Details (optional)
4. Click **Save**.

## Changing a User Type

To Change a User Type:

1. Go to **Users > User Management**.
2. Select **Edit** from the Actions list next to the name of the User and click **Go**.
3. Select the new **User Type** from the list. Fill in the User's Contact Details (optional).
4. Click **Save**.


Copyright © 2011, Juniper Networks, Inc.

# Sessions Monitoring

The **Users > Session Monitoring** page shows a table that contains tracking information of all the known sessions.

## Sessions View

The Sessions Table shows useful details about all the client's known Authentication, Accounting and Proxy. Both active and completed sessions are displayed, but they are differentiated by a visual flag.

The main columns of this table are:

- **User Name**- The values in this column are hyperlinks to authentication details and accounting history based on user name.
- **MAC Address** - The values in this column are hyperlinks to authentication details and accounting history on a separate pop-up, where the details for the current sessions and historical information such as total connects, data transferred and timestamp information are displayed.
- **Tracking Reason** - Any of the following can be displayed:
  - Standard Authentication
  - MAC Authentication
  - Bonded MAC Authentication
  - Bonded Authentication
  - Accounting
  - Proxy
- **SSID** - lists the SSID name
- **Location/AP Info** - If there is no locale or LA-200 information available, this column displays the MAC Address of the last AP.
- **Last Updated** - this column displayed the last date the session was known to be active.
- **Status** - This column provides a status description and a visual indicator of the session status, based on the last updated date.

| Flag Color | Session Status |
|---|---|
| **Green** | The session is considered still Active. This covers the following scenarios:<br>-The session is tracked by Authentication or Proxy and the last updated date is not older than 7 days<br>-The session is tracked by Accounting, an Accounting stop packet was not yet received and the last updated date is not older than 7 days |
| **Yellow** | The session status is unknown, so it is considered Idle. This covers all the sessions for which the last updated date is older than 7 days. |
| **Red** | The session is Completed. This covers the scenario in which the session is tracked by Accounting and a Stop packet was received. The session can also be Dynamically Disconnected, if a RFC 3576 disconnect message has been successfully sent to this user and there are no latest updates. |

The **Details** section provides the following information for each entry based on the last available session information:

- **VLAN**- Shown for Accounting tracked sessions only
- **Client IP Address**- Shown for Accounting tracked sessions only
- NAS IP Address

Copyright © 2011, Juniper Networks, Inc.

- **User Type** - Shown only if the user exists in the local users database so SmartPass can locate an associated User Type.
- **Last Run Access Rule** - This detail provides the name of the last run Access Rule, the event that triggered it (authentication, accounting start, accounting update, location change, roaming, manual run or scheduled run) and the event timestamp.
- **Run Proxy Rule** - This detail is shown only for sessions forwarded to another RADIUS Server by a local proxy rule.
- **Location History** - Displays the last three locales where the session has been associated. This detail is not shown for Authentication tracked sessions, because only the last authentication request is stored. For Accounting tracked sessions, the Location History detail is displayed only if SmartPass knows at least two different locations where the session was associated.

## Filtering

The table also provides a filtering mechanism, with two levels of complexity - basic and advanced.

### Basic Filters

The basic level requires the user to enter a text in the input field located in table header and click on **Filter**. The table entries are refreshed so that only those entries which contain the specified keyword as part of any column or detail are displayed.

When the user filters the Sessions table, a new option, **Remove filter,** is activated which can be used to get back to the unfiltered state of the table.

The search is not case sensitive and supports wildcards at the end of the word. A valid search text example and its search result are shown below:

After clicking on **Filter.**

Each time the user changes the filter pattern and clicks **Filter**, the new filter is applied to all the existing entries, not only to the visible table. If an advanced filter is set the Basic Filters options are not rendered until the Advanced filter is removed. If the filtering operation generates no results, the user sees only a page containing an informational text and **Remove filters**. The user can click **Remove filters** to return to the unfiltered state of the page.

### Configuring Advanced Filters

You can configure advanced filtering criteria by clicking on the **Advanced** button. This actions opens a **Advanced Filters** pop-up window.

From this page, you can select a search mode:

- **Search for sessions which match ALL the following conditions** - If this mode is selected, a session is checked against all the defined conditions. If one of them does not match, the session does not pass the filter criteria.
- **Search for sessions which match ANY of the following conditions** - If this mode is selected, a session is checked against all the defined conditions until the first match is found. If any session matches, the session passes the filter criteria.

The filters that can be used to filter the sessions are shown below:

After defining the filters click **Save**. You are redirected to the main page, which should now contain only those sessions that match the conditions.

Clicking **Cancel** from the Advanced Filters window redirects the user to the main page without saving changes.

The Sessions monitoring table header also displays **Remove Filters**, which clears the query string if the basic filter mode was used, or resets the conditions, if the advanced filter mode was used.


Copyright © 2011, Juniper Networks, Inc.

## Disconnect Sessions

You can select one or more sessions from the Sessions Monitoring Table and then select the **Disconnect**.

The Disconnect action results are shown in a new page. The results contain two tables, **Successful Disconnects** and **Failed Disconnects**, which are populated in real-time.

The action automatically produces a refresh of the main table, so that the disconnect request results could be reflected in the sessions status. If a session is successfully disconnected, it is marked as Dynamically Disconnected.

## Reports

### Accounting Summary Report

The Sessions table also provides Report capabilities to let the user report one or more particular sessions. The report is be generated as a HTML file, and has the same appearance as the existing SmartPass User Details in RingMaster.

The Sessions Details table report contains the following columns:

- Client MAC Address
- User Name
- Client IP
- NAS IP
- Location
- Reason for which the session is tracked
- Session Started
- Session duration
- Bytes Received
- Bytes Sent
- Status
- The last three Access Rules run against this session.

## Displaying User Name Report

For each entry of the Sessions Monitoring table, the user-name is linked to a detailed history report. This contains both authentication and accounting details if available.

The Last Authentication Details section shows relevant information about the last known successful authentication performed by clients using the specified username. The attributes taken into account are listed below:

- MAC Address
- Authentication Date
- Local Authentication
- Authentication Type - shown only if Local Authentication has the value of Yes.
- Run Proxy Rule - shown only if Local Authentication has the value of No.
- NAS IP
- NAS Port Identifier

The Accounting History table shows relevant information from all the accounting packets stored in the database which have a user- name attribute with the specified value. This table contains the following columns:

- Login Date
- Client MAC Address

Copyright © 2011, Juniper Networks, Inc.

- Client IP Address
- NAS IP Address
- SSID
- Location
- Session Duration
- Bytes Sent
- Bytes Received

The table footer displays the sum of duration, bytes sent and bytes received for all the table entries.

## Displaying the MAC Address Report

The MAC Address for each entry of the Sessions Monitoring table is linked to a detailed history report. This report contains both authentication and accounting details.

The Last Authentication Details section show relevant information about the last known successful authentication performed by clients with the specified MAC Address. The table footer displays the sum of duration, bytes sent and bytes received for all the table entries.

## Table Refresh

There are two ways to refresh the Sessions Monitoring table:

- **Manual Refresh** - Click **Refresh** at the top of the table.
- **Automatic Refresh** - The automatic refresh period is 180 seconds.


Copyright © 2011, Juniper Networks, Inc.

# Network Access Rules

SmartPass allows users to control access to the network based on authentication and also on physical location, accounting, VLAN information and time of day. The Access Rules tab integrates all this information enabling you to create, manage and schedule the rules. Access Rules are created using the Access Rules wizard, a 5-step process which quickly and easily filters sessions that you can change or specify which user is denied access to the network.

You can use either the **Custom Access Rule** or **Use a template** option to begin your Access Control Rule.

## Custom Access Control Rule Example

The following example demonstrates creating a **Custom Access Rule** using the Custom Access Control Rule Wizard.

1. Click **Custom Access Rule**. The template option disappears and **Step 1 of 5** for **Custom Access Rule** is displayed.
2. Click **Next**.
3. In the **Access Rule Criteria** section, select the appropriate conditions that the user session must match. Notice that the selected conditions populate the **Step 2: Edit the rule description (click a link below)** section.
4. Click the linked conditions in the **Step 2: Edit the rule description (click a link below)** section and type in or select your desired information in the dialogue boxes.

### Selecting the Conditions Descriptions

   a. **User Name Pattern** — enter a User Name pattern used to match the User Name of a client. Click **OK.**
   b. **Rule SSID Condition**— enter a SSID Name to match the SSID for a client connection. Click **OK**
   c. **Specify a VLAN Name**— enter a VLAN Name to match the VLAN of a client. Click **OK**.
   d. **Rule User Type** — select a User Type to match the User Type of a client. Click **OK.**
   e. **Select one or more locations —** the location and a condition to match the location of a client. Select one or more **Available Locales** and move them to **Selected Locales** using the arrow tools. Click **OK**.
   f. **Select a Time of Day Interval** — the time of day SmartPass runs Access Rules. Click **After** or **Before** boxes to make fields available and enter times. Click **OK**.
   g. **Specify a Traffic Limit** — the type of traffic to account for and a maximum traffic limit. Click **OK.**
   h. **Specify a Throughput Limit** — the type of traffic to account for and a maximum throughput limit. Use the traffic and throughput limit options to set throughput limits. Click **OK.**

5. Click **Next** to proceed to Step 3 of 5. Note that at anytime you can click **Back** to review or edit your previous Access Control Rule selections.
6. In the **Step 1: Select Trigger(s)** section, select the trigger(s) that prompt a check to be performed by SmartPass in the following conditions:
   - **on authentication** — updates are triggered by authentication of the user against the database.

Copyright © 2011, Juniper Networks, Inc.

- **on location changes** — updates are triggered by location change reports from the LA-200.
- **on roaming** — accounting updates are triggered by roam events (clients moving from one AP to another AP) generate on the MX.
- **on accounting start** — updates sent from the MX are triggered based on accounting start at the beginning of the session.

Notice that selected triggers populate the **Step 2: Edit the rule description (click a link below)** section.

7. Click **Next** to proceed to Step 4 of 5.
8. In **Step 4 of 5** select the changes to apply to the client session once an Access Control Rule is triggered. You can perform the following:
   - **Deny Access** — access to the network is immediately denied when an Access Control Rule is violated.
   - **Change Authorization Attributes** — select Authorization Attributes that alter the client session's attributes once a Access Control Rule is violated. For more information about Authorization Attributes, refer to the "Configuring AAA for Network Users" chapter in the *Mobility System Software Configuration Guide.*

   In this example, the **Change Authorization Attributes** option is selected. A list of **Authorization Attributes** appears in the **Step 1: Select action section** once you select the **Change Authorization Attributes** option.
9. Select **Authorization Attributes** for the client session to change. Notice that selected conditions populate the **Step 2: Edit the rule description (click a link below)** section.
10. Click the linked conditions in the **Step 2: Edit the rule description (click a link below)** section and type in or select your desired information in the dialogue boxes.

When changing Authorization Attributes for **change the Input Filter Id to a value**, always type the Input Filter Id in the form of "ACL-name." The "ACL-name.in" form is not required. The name of the ACL or QoS profile should match the name configuration in MSS.

11. Click **Next**.
12. You can type in a **Rule Name** for your **Access Rule** and add optional **Description Text** if desired.
13. Select **Activate** to activated Access Rules immediately.
14. Click **Finish** to save your Access Control Rule or **Back** to edit or review your previous selections. If you click **Finish**, the **Access Rules Management** screen is displayed. Your Access Control Rule is now saved.

## Managing Access Rules

You can view and manage saved Access Rules using options in the **Actions** list.

1. Go to **Access Rules > Access Rules Management**.
2. Click **Show** to view the details of the selected Access Control Rule.
3. To manage the Access Rules, select an option from the list of **Actions** and click **Go**.

   The following options are available:
   - **Deactivate** — this option immediately deactivates the Access Rules.
   - **Run** — this option immediately initiates the Access Rules that match the client session.


Copyright © 2011, Juniper Networks, Inc.

- **Schedule** — this option displays the **Scheduler** menu where you can set predetermined times to run the Access Control Rule instead of waiting for triggers to be activated.
- **Edit** — this option returns you to the Create Access Control Rule steps.
- **Delete** — this option deletes the Access Control Rule.

Copyright © 2011, Juniper Networks, Inc.

Copyright © 2011, Juniper Networks, Inc.

# RADIUS Proxy

RADIUS Proxy is the ability for a RADIUS server to seamlessly forward RADIUS authentication requests to an external RADIUS server, retrieve the authentication response, optionally post-process any authorization attributes, and send them back to the NAS. SmartPass specific intelligence (such as client location) has been added to the authentication response received from another RADIUS server, by leveraging its existing Access Rule framework.

## RADIUS Proxy Settings

The following are generic settings that apply to RADIUS Proxy:

- Default prefix realm separator (default value "/")
- Default suffix realm separator (default value "@")
- RADIUS Server Group fail-back retry count (default value 3 times)
- RADIUS Server Group fail-back timeout (default value 5 seconds)

## Proxy Filters

SmartPass is able to determine whether to forward an authentication request to another RADIUS server based on the conditions defined in a Proxy Filter. A proxy filter functions similarly to an MSS Authentication Access Rule. The proxy filter tells SmartPass which RADIUS servers to forward incoming requests to based on certain attribute values in an incoming request. When an incoming request is forwarded to a RADIUS server, the server authenticates it and provides a list of authorization attributes. That same proxy filter may also apply a set of pre-defined default VSA values on top of the received authorization attributes.

## Forwarding Conditions

A forwarding condition represents a name-value pair, in which the name represents an attribute that is part of a RADIUS authentication/accounting request, and the value is a generic value or list of values. A proxy filter may be defined using multiple forwarding conditions, but there may only be one forwarding condition for any distinct attribute name part of an incoming RADIUS request.

When an incoming request is received by SmartPass, it is matched against every configured proxy filter by comparing the attribute values that correspond to each forwarding condition. If all forwarding conditions in a proxy filter are matched against the referenced attributes in the incoming request, SmartPass applies the proxy filter based on the configured RADIUS Server Groups.

The following forwarding conditions can be configured for a proxy filter:

| Condition Name | Value Description | Pass Criteria |
|---|---|---|
| **User Name** | A User Name pattern, which can contain the asterisk ("*") wildcard, e.g. "JUNIPER*". | The user name, which is part of an incoming request matches against this wildcard-based user name pattern. |
| **SSID Name** | An SSID Name pattern | The SSID Name part of an incoming request matches in case sensitive mode against this pattern. This pattern is also wildcard sensitive. |

Copyright © 2011, Juniper Networks, Inc.

| | | |
|---|---|---|
| **AP MAC Address** | Any of the following value definition styles:<br>▯ A set of Vendor OUI prefixes<br>▯ A MAC Address pattern, which can contain one training asterisk ("*") wildcard, e.g. "00:11:22:*"<br>▯ A MAC Address | The AP MAC Address defined in the incoming request:<br>▯ belongs to any of the specified Vendor OUI prefixes<br>▯ starts with the MAC prefix preceding the "*"<br>▯ matches the MAC Address value |
| **Realms** | An optional list of realms. | The realm of an incoming request is part of the list. |

## Forwarding Destination

A forwarding destination is a RADIUS server group that is based on where and how SmartPass determines to send each authentication request.

## RADIUS Server Groups

A RADIUS server group represents an ordered list of RADIUS server entries and is identified by a unique RADIUS server group name. The maximum number of configurable RADIUS Server groups is eight.

## RADIUS Server Entries

A RADIUS server entry describes a RADIUS server, as a potential home RADIUS server. Each RADIUS server entry has a unique RADIUS server entry name and is described by the following configurable attributes:

| Attribute | Description | Default Value |
|---|---|---|
| **Entry Name** | A unique non-empty name, which graphically identifies this RADIUS server entry. | An empty string. |
| **IP Address** | The IP Address of the corresponding RADIUS server | An empty string. |
| **Shared Secret** | The shared secret of the corresponding RADIUS server | An empty string. |
| **Authentication Port** | The authentication port of the corresponding RADIUS server | Number "1812" |
| **Accounting Port** | (Optional) The accounting port of the corresponding RADIUS server. | Number "1813" |

The combination of IP Address, authentication port and accounting port results in a unique RADIUS server entry. Only one RADIUS server group may be associated with a proxy filter. The maximum number of RADIUS Servers per group is eight.

## Failback Capability

When SmartPass is prompted to forward an authentication request based on a proxy filter, it goes through the associated RADIUS server group entry and attempts to send the request to the first corresponding RADIUS server. If that request times out, another attempt is made with a second RADIUS server of the same group. This process continues until a RADIUS server responds with a positive or negative authentication response.

If the authentication request times out for all RADIUS servers corresponding to the RADIUS server group, SmartPass checks the “Use SmartPass as a backup server” forwarding rule setting. If this setting is ON, then it processes the authentication request locally. Otherwise, access is denied.

SmartPass stops sending the authentication request as soon as one of the RADIUS server replies or until all RADIUS servers belonging to the RADIUS server group have attempted to authenticate and have all timed out.


Copyright © 2011, Juniper Networks, Inc.

## Default VSA Values

Once an authentication request is sent to one of the RADIUS servers associated to a proxy filter and an “accept” packet is received, the next step it to check the list of default VSA values associated to this proxy filter. SmartPass adds an entry for every VSA which is not part of the authorization attributes retrieved from the authenticating home RADIUS server. The entry value is defined as part of the list of associated default VSA values.

## Realms

A realm represents a Domain Name (like identification within an authentication request). A realm is the part of a user name. For example, if a user name is jsmith@trpz.com, the corresponding realm is trpz.com. Multiple realms can be part of a user name- this indicates an expected RADIUS server route. For example, if a user name is jsmith@abc.com@ trpz.com, the first RADIUS proxy in the chain forwards the given authentication request to the RADIUS server corresponding go the trpz.com realm, which then forward the received authentication request to the RADIUS server corresponding to abc.com.

## Suffixed Realms

A common way to specify realms as part of a user name is by suffixing them to the user name by using the "@" separator. Any number of realms can be specified, where the first realm specifies the destination home RADIUS server, the second realm represents the last RADIUS Proxy server in the path and so on. The last realm specifies the next RADIUS server in the path. RADIUS clients may also use other realm separators, such as "%".

## Prefixed Realms

Another way to specify realms is by prefixing them to a user-name by using the "/" separator. Multiple realms can be used with the same ordering as with suffixed realms, e.g. "itc.trpz.com/trpz.com/nbadiu" has the same meaning as "nbadiu@itc.trpz.com@trpz.com".

Prefixed realms can be used in conjunction with suffixed realms as well, e.g. "itc.trpz.com/nbadiu@trpz.com".

Similar to suffixed realms, SmartPass can recognize configured prefixed realm separators, while a system-level default "/" separator is used. For each RADIUS proxy rule, a custom separator is able to be configured or the system-level one is used by default.

By default a RADIUS Proxy rule only looks for suffixed realms. The reason is to avoid misinterpreting machine authentication requests, where the "/" separator is used with a different meaning, e.g. "host/machine-name.domain-name". An option is provided for a RADIUS Proxy rule to also look for prefixed realms based on the default or a custom separator.

## User Name Processing

SmartPass automatically extracts the realm name from a user name when it applies a realm-based RADIUS Proxy rule.

For example, if the incoming User Name/Identity Response is "nbadiu@itc.trpz.com@trpz.com", the User Name that will be checked against the User Name Patter "nbadiu".

For non-realm based RADIUS Proxy rules - i.e. rules without a realm condition, the user name is not processed before checking it against the configured user name pattern.

## Access Rule Integration

If SmartPass forwards an authentication request to a RADIUS server based on a proxy filter and receives a successful authentication response, it first applies the default VSA values associated to the same proxy filter and then allow the authentication request to go through the Access Rule engine.

Since this is basically an authentication related event, SmartPass checks all Access Rules configured to be triggered at authentication time against the original authentication request coming

Copyright © 2011, Juniper Networks, Inc.

from a NAS. Once all Access Rules have been checked, SmartPass compiles a final response to be sent to the requesting NAS, which will be one of the following:

1. A successful authentication with the same authorization attributes as sent by the home RADIUS server.
2. A successful authentication with additional VSA values specified by the forwarding proxy filter.
3. One of the above successful authentication response with additional VSA changes performed by one or more authentication-based Access Rules.
4. A rejected authentication based on one or more authentication-based Access Rules.

## Granting Access

If SmartPass grants access based on the decision made by a home RADIUS server, it also ensures that all subsequent “Start” and “Stop” packets received for this session are forwarded to the same home RADIUS server. Note that the decision for which home RADIUS server be chosen at the time when an accounting-start packet arrives is not made based on an existing Forwarding Proxy rule. Instead, this decision is based on a temporary list of successfully authenticated sessions which were granted access by a home RADIUS server by means of a Forwarding Proxy rule. Based on the unique session ID, SmartPass knows whether the accounting packet refers to a “Proxied” session and if that is the case, it forwards the “Start” and “Stop” packets to the same home RADIUS server that performed the original authentication.

## Denying Access

If SmartPass denies access against the decision of a home RADIUS server, an accounting packet named “Proxy-Stop” is sent to the home RADIUS server. The “Proxy-Stop” packet is needed because a home RADIUS server usually expects a “Start” accounting packet as a follow-up to a successful authentication.

## Compatibility

The RADIUS Proxy functionality is compliant with the following RADIUS servers:

1. Microsoft Internet Authentication Service (IAS)
2. Juniper Networks Steel-Belted RADIUS server (SBR)/Funk
3. FreeRADIUS
4. Radiator RADIUS server

## RADIUS Proxy Tab

The new SmartPass 7.6 RADIUS Proxy tab allows the user to configure and update all the Proxy settings from one area.

The left menu contains three sections:

- RADIUS Servers Management
- Proxy Rules Management
- Proxy Settings

## RADIUS Proxy Settings

These settings are available for editing in the RADIUS Proxy Setting menu:

- A system-level realm prefix separator, "/" is default
- Asystem-level realm suffix separator, "@" is default
- A retry count value, 2 is default
- A timeout value, 3 seconds by default


Copyright © 2011, Juniper Networks, Inc.

## RADIUS Servers Management

This page displays two lists: one for any configured RADIUS Servers and one for configured RADIUS Server groups. Each table entry is editable. If there are no configured RADIUS Servers or RADIUS Server Groups, only the RADIUS Servers area will be shown. The text alerts the user that a new RADIUS server entry must be added in order to populate the list.

If one or more RADIUS Server entries exist, the **RADIUS Servers** area is displayed.

If at least one RADIUS Server Group exists, the **RADIUS Servers Groups** area is populated.

## Creating a RADIUS Server

A new RADIUS server can be created by clicking **Add** located under the **RADIUS Server** table.

The user also has the option to automatically create a RADIUS Server group and associate it to the currently configured server. The **Create Associated Group** is OFF by default. When checked, the **Group Name** is automatically filled in with the server name plus "-group".

All the fields shown below are required. If one or more fields have incorrect values, an error message is displayed and the user is be able to save the configuration.

The **Accounting Port** field displays an additional descriptive message placed in an asterisk footnote that states the following: “This information is only used for authentication related RADIUS Proxy operations.”

## Editing a RADIUS Server Entry

Each RADIUS Server entry is editable. The **Edit RADIUS Server** page looks similar to the **Create RADIUS Server** page, but the **Name** field is read-only.

## Creating a RADIUS Server Group

The **Create RADIUS Server Group** wizard can be started by clicking **Add** located under the **Radius Server Groups** table.

The wizard requires that you type a name, description, and an ordered list of associated RADIUS Servers. The defined order of RADIUS server is considered when forwarding authentication requests.

The **Description** field is optional. If a **Name** is not correct or there are no selected RADIUS Servers, the user will not be able to save his configuration.

At least one RADIUS Server needs to be selected at this stage before creating a RADIUS Server group.

## Deleting a RADIUS Server Entry

Users are asked to confirm the action to delete a RADIUS Server entry. A Web page opens with information connected to the RADIUS Server and what group is affected if the server is deleted.

If deleting a particular RADIUS server means that at least one existing RADIUS Server group will have no members, a warning message is presented to the user. The warning message explains that the impacted RADIUS Server group(s) must also be removed if they want to proceed with this operation.

## RADIUS Proxy Rules Management Page

This page displays a list of all configured forwarding rules. You can change the rules priority by using the “Move up” and “Move down” arrows.

## Creating a RADIUS Proxy Rule

Click **Add** at the bottom of the Rules table to display the “Create RADIUS Proxy Rule” wizard.

Copyright © 2011, Juniper Networks, Inc.

## Template /Custom Rule

The first page of the wizard allows you to begin creating a Proxy rule based on a template or create a custom rule. This page is similar to the first page of the “Create Access Rule” wizard.

By default, a template selection opens. There are three possible templates that can be displayed below. A description box at the bottom of the page allows an user to configure and view the complete description of his or her RADIUS Proxy rule as selections for the template are made.

If you select create a Custom RADIUS Proxy Rule, the first wizard page displays the following options:

## The Rule Conditions Page

The first page of the wizard can be skipped without specifying values for all conditions associated to the template. The second wizard page lists four conditions to select:

You can click on any of the description links to open a pop-up window, which allow you to configure a value for the corresponding condition.

## User Name Pattern

Enter a **User Name Pattern** when prompted when editing the RADIUS proxy description.

## The AP MAC Address Selection

The AP MAC Address selection page displays the following information:

After a selection is made and you click OK button is pressed, in the case of multiple MAC Address selection, the "Step 2: …" box displays a show/hide link, which allows an user to see all selected/ specified MAC Addresses.

## Selecting a Realm

The Realms selection page:

This window includes the following options:

1. A check box (unchecked by default) to allow the override of the default suffix separator. The selection will enable the following field:
   - A one-character text-field, which contains a realm suffix separator
2. A check box (unchecked by default) to allow the processing of prefixed realms, which enables the following field:
   - A check box (unchecked by default) to allow the override of the default prefix separator, which enables the following field:
   - A one-character text-field, which contains a realm prefix separator.

In the case of multiple realms selection, after a selection is made, click **OK** and the "Step 2:" box displays a show/hide link, which allows an user to see all specified realms.

## The Destination Page

Once you have specified values for all selected conditions, you can advance to the third wizard page. This page allows you to select the destination RADIUS Server group.

The user can also use the local SmartPass Server as a failover home server. In this case, if none of the RADIUS servers from the selected RADIUS server group can be reached, the requests are handled locally.

You can also opt to remove a realm that is part of a matching authentication request before forwarding the request to one of the specified RADIUS destinations. By default, any realm that is


Copyright © 2011, Juniper Networks, Inc.

part of a User Name is stripped before forwarding the request, since SmartPass acts as a RADIUS Proxy and makes decisions based on the realm. You can change this behavior by unchecking the corresponding check box.

As the user changes the forwarding destination or the other optional settings, the Rule description is updated based on his change, as shown below.

## The Default Attributes Page

Once you have selected at least one RADIUS server group, you can continue to the “Default Attributes” page.

After a User Type is selected, **Import & Overwrite** is enabled. **Import & Overwrite** allows you to confirm the User Type selection. All VSA values are copied from the selected User Type. The user’s selection of a value for Start/End Date Duration attribute determines an end-date based on the start-date (either from the authentication response or from the default start date on this page). If an end-date is already configured, the earlier of the two dates is used in the authentication response.

## The Description Page

The next page allows you to provide a name for this RADIUS Proxy rule and an optional textual description. If one or more attributes are selected in the “Default Attributes” page, each attribute is listed in the rule description box

Copyright © 2011, Juniper Networks, Inc.

Copyright © 2011, Juniper Networks, Inc.

# Maintaining SmartPass

SmartPass logs traffic and accounting messages into a database. For each entry, information in several fields are logged, including traffic statistics and client information. You can query accounting data, filter activity, and user information using log filtering capabilities which have to been expanded to include **RADIUS Authentication, Access Rules, RADIUS Proxy, Web Portal Authentication**, **RADIUS Accounting, Location Appliance, ALL, Access Control, RADIUS DAC, Coupons, RADIUS Server**, **RADIUS DB**, and **Web API** options. The information saved in the logs can help you understand how the system works and assists with troubleshooting.

1. Click **Maintenance**.
2. Select from any one of the **Server Log Module and Server Log Level** and **Filter by Log Module**, **Filter by Log Level** menus for filter options.
3. Examine log results or export log files.

## Exporting Log Files

To export log files from SmartPass, follow these steps:

1. Click **Maintenance**.
2. To review the current list of log files, click **Log History**.
3. To review a log file, click **View** next to the log file in the list.
4. You can export the log file entries based on severity. You can also query accounting data, filter activity, and user information using log filtering capabilities which include RADIUS Authentication, Access Rules, RADIUS Proxy, Web Portal Authentication, RADIUS Accounting, Location Appliance, All, Access Control, Radius DAC, Coupons, RADIUS Server, RADIUS DB, and Web API. From the **Export by module** list, select one of the filters from the **Export by module** list.

Copyright © 2011, Juniper Networks, Inc.

5. Select your desired **Export by Severity** and **Export by Module** options from the drop down boxes and click **Export**.
6. In the **File name** field, type a file name for the exported log file.
7. Type in a **File Name** and click **Create .cvs file** to save the file.

## Database Backup and Restore

SmartPass 7.6 has a database backup and restore functionality. The following tasks are now available:

- Backup the database manually
- Schedule automatic backups
- Restore the database from an existing backup

This feature is located under the **Maintenance** menu and is visible for Administrators only, under any type of license.

SmartPass supports two types of backups:

- **Manual** -Manual backups are stored at the following server location:

  `<INSTALL-DIR>/backup/manual`
- **Automatic** - Automatic backups are stored at the following server location:

  `<INSTALL-DIR>/backup/auto`

The backup files are zipped and have unique auto generated names, based on the creation date timestamp. The name assigned on manual creation is displayed only in **Backups Management** table, but it is not used as the actual file name.

The zip file contains copies of the files located under the smartpass-db directory.

You can select from creating a full or partial backup. A full backup saves the entire database structure and all the table content. A partial backup saves the entire database structure but does not store the content of the tables related to the following information:

- Authentication Request Data
- Accounting Packets Data
- SIP Data
- Access Rules Usage Information
- Proxy Rules Usage Information

## Auto-Backup

If you are logged in as an Administrator you have the option of enabling automatic generation of backups at a configured time interval using the configurable **Auto-Backup Settings**.

| Setting Name | Functionality Description | Default Value/ State |
|---|---|---|
| **Enable Auto-Backup** | If this option is checked, SmartPass creates backups periodically, based on the configured settings. | Enabled |


Copyright © 2011, Juniper Networks, Inc.

| | | |
|---|---|---|
| **Backup Recurrence** | The available options are "Hourly", "Daily", "Weekly" and "Monthly."<br>If the "Hourly" option is selected, a backup is created hourly.<br>If the "Daily" option is selected, a backup is created each day, at the time indicated by the "Time of Day" setting.<br>If the "Weekly" option is selected, a backup is created once a week. The exact time in a week is computed based on the "Day of Week" and "Time of Day" configured values.<br>If the "Monthly" option is selected, a backup is created once a month. The exact day and time in a month are computed based on the "Day of month" and "Time of Day" configured values. | Enabled, "Weekly" |
| **Time of Day** | Configures the time in a day when a backup is performed. | Enabled, "12:00 AM". |
| **Day of Week** | Configures the specific day in a week when a backup is performed. | Enabled, "Monday" |
| **Day of Month** | Configures the specific day in a month when a backup is performed. | Disabled, "1" |
| **Number of Backup Copies** | The maximum number of automatic backups that SmartPass stores.<br>Before creating a new backup, SmartPass tests the number of already existing backups and if it the maximum allowed value was reached, the oldest backup is deleted.<br>The allowed range of values is 1100. | 10 |
| **Include Monitoring Data** | This setting determines if the monitoring tables are included in the backup or not. The configuration tables are always included in the backup. | Enabled |
| **Save** | Save and applies the changes | N/A |

## Creating a Manual Backup of the Database

To manually create a backup at any time, follow these steps:

1. Enter a **New Backup Name** in the the **Manual Backup** form.
2. You have the option to click the **Include Monitoring Data** box to have the monitoring tables included in the backup file. The configuration tables are always include in the backup files.
3. Click **Create Backup**.

A message displays to let you know your manual backup was successful. Your new backup file is now displayed in the **Backups Management** table.

## Backups Management

The Backup Managements section has a table of all existing backups, listed from newest to oldest backup The Backups can be sorted by clicking on the header of each column..

The table columns with their content descriptions are listed below:

| Column Name | Description |
|---|---|
| **Name** | The name assigned by the Administrator at creation time, or an empty string if the backup is automatically generated. |
| **Created On** | The date and time when the backup was created. |

Copyright © 2011, Juniper Networks, Inc.

| | |
|---|---|
| **Created By** | The name of the Administrator who created the backup, or "SmartPass"if the backup was automatically created. |
| **Version** | The product version when the backup was created. |
| **Backup Type** | "Manual" or "Auto". |
| **Contents** | Can have the value of "Configuration, Monitoring" if the backup was created including monitoring tables, or "Configuration" in the opposite case. |

The table allows single selections and has an **Actions** menu on top. Users can chose from the following **Action** options:

- **Restore** - The user is asked for a confirmation of his “Restore” selection and, if received, the SmartPass database and configuration file is replaced with the selected backup.
- **Download** - The user can download the backup file from the SmartPass server and save it using a custom name.
- **Delete** - Deletes the selected backup.


Copyright © 2011, Juniper Networks, Inc.